Final Report

40 Credits	CM3203 One Semester Individual
Author	Samuel Maltby (C1334821)
Supervisor	Jianhua Shao
Moderator	Hontao Liu
Project Title	Fabricated Profiles on Social Media Platforms.
Special Provision	Dyslexia

Abstract

The fabrication of Facebook profiles is an ever growing issue and many social media users are not educated on the matter. This is mainly due to the fact that the threat is a modern one, with the technique only recently being discovered by cyber criminals. With Facebook regularly updating and creating new and interesting aspects to its service, the ease for users to unwillingly and unintentionally expose themselves is expanding.

The initial part of this project involved researching previous studies on fabricated profiles, with particular focus on the studies relating to Facebook. Following this research, primary research was undertaken in the form of a questionnaire and interviews. The questionnaire returned 118 responses and significantly aided the testing of the hypotheses. The outcomes of the questionnaire were a key deliverable for this project.

The second part of the report focused on developing a risk measurement tool. This measurement tool was used to educate Facebook users on the specific content of their profiles that increased their risk of becoming a victim, additionally outlining the attacks that they were particularly vulnerable to.

Overall, the outcomes of the primary research conducted by this project suggest that social media users need further education on the risks posed by fabricated profiles, and how they can prevent the likelihood of their own victimisation.

Acknowledgements

Firstly, I would like to thank Dr J. Shao for his continued input, knowledge and enthusiasm throughout my project. I would like to thank him for the ideas that he has suggested throughout, and for inspiring me to complete this project to the highest possible standard.

I would also like to thank all of the respondents that participated in the project's research. Without these respondents, this project would not have been possible. I would also like to give a special thanks to the five subjects that participated in the risk measurement tool evaluation. With the process requiring screening on profiles, I am appreciative that the subjects entrusted me with their account content.

Finally, I am thankful to all of my family and friends for their continued support throughout the project, with special thanks to Laura C for her ongoing encouragement and motivation.

Table of Contents

Table of Figures

Introduction

Social media platforms are continuously growing in popularity and are becoming a requisite feature of many people's life. Facebook is defined as a social media platform and requires no cost for use of the service. Once registered, users are able to post a wide variety of information in many different formats. These include, but are not limited to, uploading a status, publishing a photo and broadcasting life events. The most popular method is by uploading a status which holds a string of information. Many users often abuse this feature by uploading information which contributes to defining the individual and helps strangers understand their behaviours and attitudes. A study carried out by Statista (2015) shows that the number of active global monthly users is 1.59 Billion, revealing an increase of 360 million users since 2013.Facebook have openly announced that they are unable to determine the differences between a legitimate and false profile. In the Facebook Annual Report (2013) they suggested that up to 11.2% of their monthly users were indeed fake.

This paper will focus on Facebook as a social media platform and will determine whether users are aware of the increasing threat of fabricated profiles. This will be demonstrated by discovering what the public think about their online profile privacy, and if they are satisfied with the current measures and precautions Facebook have implemented to tackle the problem of false profile creation. Furthermore, the paper will investigate whether people harm their personal security through frequent use of social media by screening profiles against commonly used security questions that can gain access to bank accounts, emails and any account that is accessible online. These results will then be presented to the user to discover whether their attitudes have changed. When presenting the results to the user, personal implications will be shown. This will increase the chances of them changing their attitude as the project's results will directly affect the individual.

The paper will attempt to prove or disprove multiple assumptions with the aid of extensive independent research. The project will be initially supported by related work to give a strong foundation to any assumptions made. Questionnaires, interviews and profile screenings will be carried out in order to achieve these aims and will use a pre-defined risk assessment which will be produced independently by the author of this report.

Furthermore, I will implement prototypes in the form of wireframes that Facebook can implement to increase awareness to their users of the risks associated with each piece of information they upload to their network of friends. The hypotheses for the project are as follows:

- (**H1**) The older generation (40+) have spent more time understanding the privacy policy developed by Facebook compared to the younger generation of Facebook users (18-39).

- (**H2**) Young people are more ignorant with regards to privacy and over exposure on social media platforms, but are more likely to be aware of the privacy settings in relation to their account compared to the older generation.

- (**H3**) Facebook users with relaxed privacy settings are more likely to be approached by a Fabricated user.

- (**H4**) Social media users do not fully understand the growing risks of fake profiles and threats that fake users can impose on innocent users.

- (**H5**) Social Media users are unaware with what information and accounts can be accessed with the information they have provided on their Facebook Timeline.

Related Work

Facebook and other social networking sites (SNS) are commonly used by a wide audience of people. Since Facebook formed in 2004, innovation has been a leading focus, with great efforts made to update features and produce new ways for users to interact and exchange information to their network. In late 2011, Facebook changed users profile space by introducing the 'Timeline'. The feature allowed users to view someone's profile and their entire content on one page, adding simplicity and efficiency to the service they provide. The introduction of new features creates distractions for underlying problems related to privacy and security. This section of the report will highlight the findings from work carried out in the area of privacy implications, reactions to fabricated profiles, and to highlight current attitudes and concerns Facebook users have with their privacy.

The public's current awareness and attitudes towards the current privacy rulings used by Facebook

Liu. Y (2011) analysed the trend between what users expect from Facebook privacy control settings with the default privacy settings currently implemented by Facebook. In his report, it suggested that 36% of Facebook users had not observed their privacy settings and used Facebook's default framework. The sample size for Liu's survey was 200 random Facebook users which varied in age and gender. Only 74 respondents said that the default privacy settings matched their expectations and that they would be comfortable continuing their social activities. The privacy settings that Facebook previously used as a default were to make the account public, meaning that anyone with an account could openly access other profiles and observe what information they were uploading. Liu. Y (2011) deduced that users were becoming increasingly unaware of Facebook's privacy settings, with over 50% of users uploading freely accessible personal content.

Magid. L (2014) documented that Facebook changed their default setting to only allow friends to access personal content. Although this was an attempt to rectify and improve the users privacy, they were only able to implement this change for new users. This means that up to 615 million active monthly users upload information and are unaware that it can be accessed publicly.

Patient Privacy Rights (PPR, 2015) provide comprehensive assessments on privacy policies which are published by market leading companies to see if they meet appropriate guidelines. Since Facebook formed, they have been doing yearly reviews which are published, as shown below.

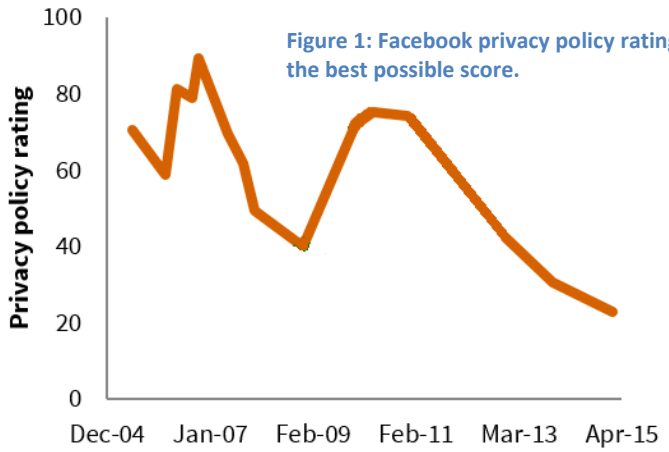

Figure 1: Facebook privacy policy rating over time as a percentage of the best possible score.

The results provided by PPR show that Facebook's privacy policy has deteriorated, becoming less transparent. As a result, PPR express that users should make every effort to read and understand the policies, as Facebook do not make any efforts to update users when changes have been made. Consequently, users become unaware to how their information is processed and treated.

The Implications of fabricated user profiles on Facebook and types of malicious attacks that have occurred under a fake profile

A study by Krombholz et al (2012) looked into the interactions between fake and real profiles. Their study outlined what information is required to create an undetected fabricated profile that users could pass off as a legitimate one. In Krombholz et al studies, eight fake profiles were created with an equal split in genders, and contained different amounts of publicly disclosed information. This information included, but was not restricted to, relationship status, interests, workplace and date of birth. After the study finished, a total of 1,083 connections were made. The assumption was that the connections were all authentic. Out of these connections, 72% were associated with the fake accounts belonging to the female gender characteristic. This statistic aids studies carried out by Barracuda Networks (2012), suggesting that 97% of fake profiles on Facebook state that they are female.

Various kinds of attacks have occurred through social media under a fake profile, the main reason being that the attacker remains anonymous. Attackers have many different intentions. These include trying to humiliate and embarrass a user by uncovering private information to a select network of friends, stalking an individual and taking advantage of their movements by blackmailing them into doing something that they are uncomfortable with, and 'Catfishing' which has had an increased threat in the past couple of years due to the popularity of online dating. Catfishing occurs when an attacker creates a profile under a false identity to pursue online relationships with unknowing targets. Once the attacker has acquired a false sense of security, they will ask for personal details or financial aid.

Over Exposure on social networking sites

With users frequently uploading information to their profile, questions will always be raised as to whether users are over exposing themselves online. Lavasoft (2013) tackled this question and produced a report discussing how users are changing their behaviours. They discuss how over exposure can dramatically affect an individual's reputation with the public purely based on their social media activities. In many cases, usually with young adults, their profiles affect their chances of securing job prospects and opportunities due to employees screening their content and deciding if they have any controversial activities or views online. A study carried out by Abine Inc (2013) states that only 16% of young adults make efforts to improve their web presence and social media footprint.

Alongside this figure, Abine also say that 60% of graduates are not concerned about their online profiles when it comes to affecting their reputation. These studies closely relate to this report's assumption that young people are ignorant with regards to privacy and over exposure on social media platforms, and do not consider the risks associated with the content that they upload to their social network.

Little information has been published to conclude when someone has over exposed themselves. Usually, over exposure is when content is shared on a social media platform that would not usually be disclosed in face-to-face communication. This information includes political views and inappropriate photos. When over exposure is defined, it will be easier to evaluate someone's profile.

A recommender system for privacy settings in social networks

Research carried out by Ghazinour K et al (2013) looked into privacy risks associated with disclosing personal information on a social media account. Their initial aims were to raise awareness of user privacy settings by providing potential risks to individual users based on their current social media privacy settings. This was possible due to the development of software called 'YourPrivacyProtector' which "allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. It monitors by providing a brief review for the users". This review was possible as the software was able to acquire user attributes via Facebook's API, (Also known as Data Harvesting) and then the results were analysed by using a pre-defined algorithm. They used a total of 150 users, mainly students, to complete this study and uncovered some interesting results. Their study showed that 88% provided their education level, with only 6% showing their degree course.

Attribute	% missing
Degree	94%
Political view	91%
Religion	67%
Relationship	39%
Hometown	36%
Interests	32%
Location	20%
Education	12%
Gender	4%
Age	0%

Figure 2: % of attributes users did not share

Although the outcomes of this report were indecisive, the research is still relevant to this project as it aims to uncover similar findings, but instead of categorising users into a privacy behaviour group, the author will be providing the user with risks relating to fabricated profiles. The technique used to complete the study will be considered when this projects risk assessment tool is developed. Figure 3 Below shows the pre defined values used when screening each subject.

Attribute	Description
Name	The user's full name. `string`.
Gender	The user's gender: `female` or `male`. 'string`.
Birthday	The user's birthday. `user_birthday` or `friends_birthday`. Date `string` in `MM/DD/YYYY` format.
Education	A list of the user's education history. `user_education_history` or `friends_education_history`. `array` of objects containing `year` and `type` fields, and `school` object (`name`, `id`, `type`, and optional `year`, `degree`, `concentration` array, `classes` array, and `with` array).
hometown	The user's hometown. `user_hometown` or `friends_hometown`. object containing `name` and `id`.
relationship_status	The user's relationship status: `Single`, `In a relationship`, `Engaged`, `Married`, `It's complicated`, `In an open relationship`, `Widowed`, `Separated`, `Divorced`, `In a civil union`, `In a domestic partnership`. `user_relationships` or `friends_relationships`. `string`.
religion	The user's religion. `user_religion_politics` or `friends_religion_politics`. `string`.

Figure 3: Attributes collected from user profiles

Facebook users easy targets for identity theft

Fabricated profiles can be created with the intention of stealing someone's identity. This is another threat that social media users face. Sophos (2007) conducted a similar study to a study carried out by Ghazinour (2013). The main difference between the two studies was that Sophos conducted their research through the use of a fabricated profile, whereas Ghazinour's study used a questionnaire. The fake profile created by Sophos used the name 'FreddiStaur' (ID fraudster re-arranged). The account requested to be 'Facebook friends' with 200 random users. According to the study, 82 users accepted the request. Below is a summary of the findings:

- 72% provided one or more e-mail addresses associated with them.
- 84% provided their full date of birth.
- 78% provided their current residential address or location.
- 87% provided their details on education or work.
- 23% provided a phone number.

Ron O'brien, a senior security analyst at Sophos, stated that "it's extremely alarming how easy it was to get users to accept Freddi" with "most people not giving this kind of information out to people on the street but their guard sometimes seems to drop in the context of a friend request on the Facebook site".

With findings similar to those discovered by Ghazinour, it was surprising to see that users were 58% more likely to expose their location to "Freddi", than they were to Ghazinour's questionnaire. From these results, it could be interpreted that students (the younger generation) are less likely upload content relating to their location. This was taken into consideration for the formulation of the questionnaire and measurement tool for this project.

Project Planning and Methodology

The author of this study will use research techniques that have been drawn from previous studies outlined in the 'Related Work' section of this document. The study will aim to investigate the awareness users have to the risk of over exposure on social media platforms, and to discover the relationship between over exposure and the level of threat presented by fabricated profiles. The main objective throughout this study is to present the author's research to selected users with the intention of positively impacting their current awareness and opinion on the subject. The objective was formulated to create greater purpose to the project by leaving impressions on Facebook users.

The study will also aim to uncover differences in attitudes between pre defined age groups. These age groups will focus around the younger generation (18-39) and the older generation (40+). By comparing age groups and analysing the research, this study will be able to determine which age group is at a greater risk and the difference in attitudes and arrogance towards the subject, which will revolve around privacy and cyber attacks which are possible due to abusing social media platforms.

As the study will be informing users of the risks associated with the content that they upload, an investigation will take place to determine the current attacks Facebook users have experienced when becoming a victim of a fabricated profile. This action is required to give the study greater depth and to ensure that the research shown to users is proven and relevant to the current online environment surrounding social media.

Data Collection

Multiple research techniques will be used throughout the study to ensure all hypotheses can be effectively analysed and concluded. Taking this step will ensure that the conclusions show quality, providing established answers to the questions and aims stated at the start of the project. Initial research in the form of a questionnaire will aim to answer many assumptions and will be the main research technique used for this study. It will allow the author to measure parameters for an age group and to determine whether users of various age groups hold similar views and awareness towards the study topic. The questionnaire will consist of qualitative and quantitative questions.

Quantitative questions, also known as a deductive research technique, will be developed to help provide evidence for a pre-specified hypothesis with the intention to either confirm or reject the hypothesis. Qualitative questions, also known as inductive research technique, will be used alongside the deductive approach to help contribute to the hypothesis and to also help indicate if the responses to the quantitative questions are legitimate. When concluding the hypothesis, Chi-squared statistics will be used to compare the expectation to the actual result. Other measurements have been considered, an example being Fisher's exact test, however the author aims to have a greater sample size which will be discussed in the next section labelled 'Sample'.

Additional techniques will be used to enhance the data collection required to develop an effective study. The initial plan outlined plans to develop a risk assessment model to analyse user awareness and the risks associated with their account. In order to ensure that this is a success, interviews will be carried out before and after the assessment has taken place. This was decided as the author is required to acquire the informants change in views and feelings as a direct result of the assessment.

Towards the end of the study, a focus group will be used. This addition to the author's data collection will help to evaluate the conclusions and try to gain an insight into why the statistics uncovered by the research exist. The focus group will also aid in developing future work ideas. All of these research techniques will ensure that sufficient efforts are undergone to create learning outcomes for the project. It will also allow users to repeat and validate the findings of the study.

Sample

When collecting samples, Google forms was used which collated all responses and allowed the author to export the raw data into additional software. The samples were collected by advertising the questionnaire on social media platforms. To ensure that no bias was reflected in the study's results, all age groups were permitted to respond and could exit the study at any stage of the project. The samples were prepared on Microsoft Excel and all graphs used to analyse the data were developed using this software product. As mentioned previously, Chi-squared was the statistical technique used as the sample size exceeded 100 people, meaning that the outcomes of this statistical measurement would be accurate throughout. Other measurements were considered to ensure that results could still be analysed effectively if the sample sized was not as expected before releasing the questionnaire. When analysing the data using Chi-Squared formula, it is expected that the results will reflect a specific distribution. When analysing the results for this study, discrete uniform distribution will be used throughout. The presumption being that all outcomes have an equal probability of occurring and this will be represented when stating the expected hypothesis (Ho).

A total of 118 Facebook users responded to the questionnaire with 5 users being shortlisted to partake in further research using FRAM (Facebook Risk Assessment Measure).

Ethics

With the project involving primary research techniques which can potentially hold sensitive information, efforts will be made to ensure that all data remains anonymous throughout the study, with no possibility of tracing the information back to the respondent. When releasing the questionnaire, the author will make it clear that respondents must be above the age of 18. As this project is focused on research, guidelines shall be followed. Bryman,A and Bell, E.(2011) collated principles of ethical consideration when creating projects. These are as follows:

1. Research participants should not be subjected to harm in any way whatsoever.
2. Respect for the dignity of research participants should be prioritised.
3. Full consent should be obtained from the participants prior to the study.
4. The protection of the privacy of research participants has to be ensured.
5. Adequate level of confidentiality of the research data should be ensured.
6. Anonymity of individuals participating in the research has to be ensured.
7. Any deception or exaggeration about the aims and objectives of the research must be avoided.
8. Any type of communication in relation to the research should be done with honesty and transparency.
9. Any type of misleading information, as well as representation of primary data findings in a biased way, must be avoided.

The author will ensure that these principles are satisfied throughout the study.

Limitations

With any research project, limitations will need to be acknowledged in order to help the author conclude the study and suggest any future work and further developments for the project. The limitations of the project are listed below:

- Social media is a new modern technology and the threat of fabricated profiles is currently poorly defined with little previous research on the topic.
- Only one statistical measure has been used to analyse primary research.
- When conducting primary research methods, all data and responses have not been independently verified.
- This research project has been constrained to a deadline.
- The risk assessment can only be completed on users who have responded to the initial questionnaire

Defining a Fabricated profile on Social Media

With this project having a main focus on fabricated profiles on Facebook, it is important to define what a fabricated profile is and the different intentions behind owning a fake profile. With social media innovating and growing at an exponential rate, it is hard to uncover the key differences between a legitimate profile and a fake one.

Cambridge Dictionaries (2016) define 'fake' as "someone who is not what or who they claim to be". When applying this definition to a fabricated social media profile, it is not always accurate.

Many owners of fake profiles have legitimate reasons for having them. These need to be understood and should not be considered when completing this project. These profiles are created for genuine personal, professional, security and creative reasons. Many users choose not to fully disclose their information on their social network. This often leads to creating two profiles, one being personal which contains friends and family outside of work, and the other remaining professional containing relevant information and restricts their network access to colleagues and people relating to their area of expertise. Although both accounts do not contain identical information, they are both categorised as authentic profiles.

The main piece of information which many professionals change is the profile's name or identity and do so with different intentions. Facebook challenged users that were intentionally keeping their profile anonymous. To counter this problem, Facebook introduced a 'real name' policy to reduce the amount of active fake profiles. This was enforced by prompting profiles to produce identification such as passports and drivers licences and was introduced shortly after Facebook was founded in response to the vast amount of fabricated profiles being created, it had the intention of reducing the threat of fake profiles.

Many professions later questioned this policy, as they used a false name without any intention of deceiving people. These professions include security or espionage, actors that are better known for their screen names and Native Americans who are put at a disadvantage when using their real name. The Independent (2015) published an article by Griffin regarding Facebook's real name policy. The article discusses the policy's intention of making people accountable for what they say, as it ensures that they cannot conceal their identity in order to "harass, bully, spam or scam someone else's". However, due to the backlash from the public, particularly Native Americans and the LGBT community, Facebook has said, according to this article, that they would employ changes that will make the "process of proving that names are authentic more transparent and easy" (Griffin, 2015).

Another approach to consider when defining a fabricated profile is when a user enters a false E-mail or phone number that they do not own when registering an account. Although there is little research or documentation in this field, it is common knowledge that when prompted for information on registration, users occasionally enter one or two false entities to avoid spam and advertisements. When this is undertaken, the profile is considered to be fake and they are not who they claim to be. With this project, these profiles will not be considered as their intentions are not threatening.

Many profiles appear fake at first glance. After acquiring understanding, it is clear that the purpose behind an account must be considered and concentration on the ownership of the account should be avoided. The definition of a fabricated profile that is relevant to this project is “The profile is not what they claim to be, using an innocent victim’s personal information to cause disruption with the intent to damage an individual's image or financial state”. The disruption and damage to an individual will be defined when developing a Facebook Risk Assessment Measure later in the project.

Current Fabricated Profile Attacks

Spambot is a common cyber-attack. Gallagher. B (2013) defines Currently there are many different reasons why a person would use a fabricated social media profile to attack an individual or to use for self-promotion. When defining a fake profile, it was concluded that not all have the same intention and many do not create a risk to the Facebook environment. As this projects aims to promote awareness over the dangers of fabricated profiles, this section will only research and highlight types of fake accounts that have the potential to attack an individual.

Catfishing

'Catfishing' is a major threat on social media platforms. It transpires in two different ways, both types affecting different individuals. It is a term used when a user attempts to seduce another individual by using their online identity. In the majority of cases, the online identity used is fake and contains no information that describes the owner behind the account. Instead, the information is generic and usually acquired by stripping someone else's identity. This is one type of attack; someone remaining anonymous using another person's personal information to seduce others. This can affect that person's reputation and integrity if they target people associated to them. The second type of attack relating to 'Catfishing' is when someone is targeted by this fake profile. A study by Hampton et al (2011) shows that Facebook users have not met, on average, 7% of the users in their friends list in person. This increases the risk of becoming 'Catfished' as the owner is unaware of these fake accounts and would struggle to verify whether these 7% are showing their real identity.

Spambot

A spambot is a program designed to harvest E-mail addresses from discussion boards, news groups and social media websites. This occurs as a result of the spambot recognising HTML expressions that present E-mail IDs, an example being '<a href="mailto: abc@123.com" a/> (underlined section showing the expression). On social media platforms, the Spambot is executed under the use of a fabricated profile, approaching users to click an external link where E-mails are extracted. This process is shown below.

Figure 4: Spambot

Cyber Stalking

Facebook allows users to 'Block communication' with other accounts. Blocking communication prevents any communication between two accounts, making them both inaccessible to one another. This action encourages the creation of fabricated profiles. Fake profiles will be able to gain access to the user that blocked the individual in the first place. This promotes stalking, whereby the blocked user can spy on the other user's activity, interacting rarely and making sure that they go unnoticed.

This attack occurs with little warning and the victim is unaware of this process. Stalking can aid greater threats towards an individual, depending on the owner of the fabricated account. Sex offenders use fake profiles to stalk users in order to acquire photos and information. Toby Dagg, a senior investigator at the eSafety Commissioner is quoted by Battersby. L (2015) saying "One paedophilia site contained more than 45 million images with half the material appearing to be sourced directly from social media". This carries a far greater threat to social media users, in particular young teens aged 13-18 and parents of young children.

Many other crimes are associated with fake profiles. BBC News (2016) released an article on the actions being taken by the Crown Prosecution Service (CPS). The CPS are advising lawyers to prosecute 'trolls' who use fake profiles to harass others. An internet troll is an individual that uses the internet to post inflammatory, off-topic messages on online communities and profiles with the intention of producing emotional responses. The reason why trolls post messages under a false profile is to keep their identity anonymous, reducing threats aimed towards them. Revenge pornography is a newly formed threat, where people upload explicit images of former partners to their social media profiles with the aim to humiliate them. CPS have categorised the crimes undertaken by cyber criminals into three categories. These are as follows.

Category 1: When online activity results in a credible threat to an individual

Category 2: When someone is specifically targeted for harassment, stalking, revenge porn towards former partners or family members.

Category 3: Cases resulting in breaches of a court order.

New threats are being undertaken through the internet due to rapid innovation and development. Saunders. A (2016), a director of public prosecutions, states "Online communication is developing at such a fast pace, with new ways of targeting and abusing individuals online constantly emerging. We are seeing more and more cases where social media is being used as a method to facilitate both existing and new offences".

Phishing

Phishing is a popular method used by cyber criminals to acquire sensitive data. 'Whale phishing' is a digital con targeting managers and self-employed people**.** Brecht. D (2016) has suggested that 95% of all attacks on enterprise networks are the result of successful whale phishing. Social media aids this threat by providing information that employees have openly disclosed. This information can be used by criminals to structure a more believable attack aimed towards the company. The criminals' objective is to plant a key logger on the user's computer. A key logger is used for surveillance and has the ability to record instant messages, E-mails and any information which is formulated from an individual's keyboard. The criminals' main objective is to uncover confidential information which can lead to further, more substantial threats. If the user of a profile is a student or unemployed, criminals can still target that user by altering their method of approach and changing the content to tailor the individual's needs.

Primary Research Method

Questionnaire Planning

This project will use different techniques and methods to collect data. Initially, a questionnaire will be produced to gather information from a large audience. This will show a variety of views and opinions on this area of study. To ensure that the correct outcome of the questionnaire is achieved, the author of this project produced main objectives to aid the questionnaire in providing appropriate outcomes and precise questions. The objectives for the questionnaire are as follows:

A. **To obtain user awareness on the current privacy measures used by Facebook and determine if the user has made any efforts to change their personal privacy settings.**

   The reasoning behind setting this objective was to gain understanding as to whether users take time to read Facebook's privacy policy, showing if efforts have been made to make accounts more secure by altering social media activities. This objective was also set to prove or disprove initial research suggesting that the standard of Facebook's privacy policy has declined since 2004 when the social media platform formed. A factor that PPR noted when scoring the policy was that the policy was not user friendly and used language to deter users from understanding key information.

   Secondly, this objective was set to acquire knowledge on whether users were aware of their current privacy settings and if any action was taken to adjust these settings to reduce the risk of outside threat, including becoming in contact with fabricated profile.

B. **To gain users' opinions on fabricated profiles by presenting statistics to gauge their initial reaction. To obtain any known experiences users have had with a fake profile and whether this changes social media activities as a result.**

   The logic behind this objective was initially increase awareness around fabricated profiles and discover recipients opinions on figures that I had uncovered from research and analysis related to previous studies. This objective also brought focus to previous user interactions with fake profiles allowing recipients to express their experiences and whether they own a fake profile. To complete this objective, the questionnaire recipients remained anonymous as constructing a fake profiles was against the current Facebook terms and conditions.

C. To effectively analyse any changes in attitudes between the younger (18-39) and older generation(40+).

This objective aims to support the project's analysis when disproving or proving the hypotheses stated in the introduction of this report.

Design of Questionnaire

In order to create an appropriate questionnaire, multiple research techniques and tools were considered. Many if these techniques were then implemented into the questionnaire design. These techniques are discussed below:

A. What style of question should be used in the questionnaire?

When designing the questionnaire, style and delivery had to be considered. The reason for this being that it is very important to retain the respondent's focus throughout the questions, making sure that they are not distracted as this would affect their answers. Due to previous knowledge on questionnaires, the author knew how to efficiently engage with the user. This was managed by using open and closed questions which were closely tied together, in turn aiding the learning process as it allows the author to gain more understanding and background. A closed question would not be able to provide the same amount of information on its own.

Three main styles were chosen for the questionnaire and were used throughout. Multiple choice questions were used to acquire basic knowledge on the users, with the questions focusing on factors such as age and gender. These were all closed questions, meaning that analysis was straight forward and efficient.

Short and long answer questions were used to allow respondents to expand on closed questions, giving them an opportunity to express their opinion and experience on the topic more openly. These questions helped to build rapport with the respondent, building and maintaining open dialogue throughout. Towards the end of the questionnaire, likert scale questions were used. This style of question allowed respondents to state whether they agreed or disagreed with pre-defined statements, also giving them the option to remain neutral if they wished to. These statements were collected from the secondary studies mentioned in the related studies section of the report. Survey Monkey (2013) suggest "The likert scale is a universal method for collecting data and provides a quantitative response, similar to multiple choice questions, allowing simple conclusions to be drawn".

Short and long answer questions provided qualitative answers. These answers require more processing to analyse but provide greater understanding, and are a very good alternative to closed questions.

B. How many questions should be asked in the questionnaire?

Consideration was taken when deciding how many questions to use in the questionnaire. This was an important factor, as it relates closely to the popularity and overall success of the project. The overall success will be judged on the quantity and quality of responses received. A conscious effort was made throughout the design to limit the time taken to complete the questionnaire for any respondent to under five minutes. This was successful, as the author kept the objectives set prior to the design in mind, ensuring that irrelevant questions were not asked and that there were no distractions.

C. Consider what language is best suited for this questionnaire?

The topic of this project could potentially be perceived as a technical one. In order counteract this perception, the author made great efforts to ensure that simple English was used throughout, also limiting the amount of specialist terminology used. Efforts were made to ensure that all of the questions had a short description attached to them, making sure that the recipient had a full understanding of what was being asked of them. Efforts were also made in order to ensure that the fonts and colours used could be understood by a mass audience.

D. What questionnaire layout will best suit this study?

It was decided that research on this topic needed to be conducted, as it carries major importance towards the design on the project. A study by Vanno et al (2011) suggested that white space needed to be considered as it "will allow the questionnaire to appear short and easy". In addition to this, white space aids in separating the questions. Vanno et al (2011) also recommended the use of headings in order to ensure that an efficient layout is created. Headings also offer greater clarity throughout. After carrying out sufficient research, the layout of the questionnaire became clear and concise. The author wanted to make sure that the content was comprehensive, whilst also making sure that the questionnaire did not exhaust recipients, as this would increase the risk of incomplete results. In order to avoid this problem, it was decided that the questions would be split into four main sections. These 4 sections were: 'About you', 'Facebook Privacy', 'Your Experience with Fake Profiles', and lastly 'Attitudes Towards Fake Facebook Profiles'. A progress bar was also provided throughout the questionnaire, informing the recipient of how much of the questionnaire they had already completed and how much they had left, keeping them constantly updated on their progress.

E. What service should the questionnaire be created with?

Initially, there was some difficulty in deciding an appropriate platform to create the questionnaire on. After research was conducted, many platforms were shortlisted, including 'SurveyMonkey', 'SmartSurvey' and 'KwikSurveys'. They all provided what was required with regards to functionality and ease of sharing. Before deciding on a platform, a collection of ideas were presented to a focus group consisting of fellow students. They all stated that these platforms were viable, but directed attention towards 'Google Forms' which is a free service. As the author has previous positive experience with 'Google', it was clear that it would be a reliable and efficient service. The company offer users all the functionality required to produce a professional survey, whilst also providing analytic tools. This was a great benefit with regards to the project as it reduced the time taken to process the data. Google products are trusted by the wider population. As a result, more people are likely to respond to the questionnaire as they know that it is reliable and trustworthy. In turn, an increase in the amount of recipients should result in more accurate data.

Questionnaire Justification

Section 1 - About you

This section of the questionnaire focused on the gender and age of the recipient taking part in the survey. This section provided a greater understanding of the demographics of Facebook and enabled the author to analyse the possibility of a correlation between age groups and the precautions taken when uploading information. It was apparent when publishing this questionnaire that the majority of respondents would be between the ages of 18-24, as they associate with the same social networks that the author is involved in. Thus, the author decided to research beliefs that young people have towards social media. Madden et al's (2013) study, titled "Teens, Social Media, and Privacy", suggests that "60% of young Facebook users keep their profiles private, and most report high levels of confidence in their ability to manage their settings". It could be suggested that this is due to the part that technology plays in young peoples' lives, and the fact that a lot of their knowledge is self taught. The study also measured changes in personal information provided by young users in 2006 and 2012. These categories include school name (22% increase), email address (24% increase) and cell phones numbers (18% increase).

To further solve this problem, a conscious effort was made to advertise this questionnaire to older age groups by using forums and online networks consisting of mature adults. This measure proved effective and assisted the analysis when concluding if there was a correlation between age and awareness towards risk of personal information.

Section 2 - Facebook Privacy

The seven questions in this section of the questionnaire all related to Facebook privacy and the settings that account holders use in order to feel safe and secure. The first question was asked in order to understand if users make an effort to read the latest privacy terms Facebook has provided. It was initially expected that the majority of recipients would state that they do not make an effort to do so. This is because Facebook makes little effort to effectively produce these documents to the user. Furthermore, the author wanted to explore what settings individuals use to make themselves and their content feel secure. The author wanted to make sure that these questions were answered based on the individual's knowledge, without accessing their personal privacy settings. The reasoning behind this was to determine whether users were firstly aware that their privacy settings could be adjusted, and secondly whether they were aware of the settings that are in place on their account. After the user had the opportunity to answer these questions based on their own knowledge, they were then asked if the questionnaire had raised awareness and had prompted them to go and view their privacy settings. Furthermore, prompting them to view their privacy settings may make them more aware of the changes Facebook have made towards its privacy policy since it was created in 2004.

Section 3 - Your Experience with Fabricated Profiles

This section explored previous user experiences with fake profiles. The author decided to split the questions into two sub sections. The first sub section asked the respondents whether they owned a fabricated profile and aimed to discover the motivations behind using one. Qualitative methods were used in this section to gain some insight into the individual's opinions. These set of questions were important, as the author wanted to compare the findings to the figures suggested by Facebook (2013), which stated that up to 11.2% of profiles are fake. Due to the sample size of this project, the findings may not be as reliable as the figures published by Facebook. However, it will provide a good insight into the topic. If the author was given more time to complete this project, the sample size could have been increased.

The second sub section asked respondents if they had been in any contact with fake profiles to their knowledge. This was included in the questionnaire to establish if the respondents had any current or previous experiences with fake profiles, and to get a better insight into the methods that people will use to deceive other Facebook users. In addition, the answers to this question enables the author to ascertain the average Facebook user's ability to detect a fabricated profile, and the most common techniques used by those fake profiles.

When analysing the questions in this section, an assumption has been made that the amount of people that own a fabricated profile will be close to the maximum figure that Facebook has stated (11.2%). In addition, the author believes that of the respondents stating that they have been in contact with a fake profile, the majority of those fake profiles will be anonymous people asking for personal information that is not provided on the user's Facebook account.

Section 4 - Attitudes towards Fake Profiles

This section provided multiple statements, as mentioned previously, using the likert scale. This technique was used for measuring attitudes, as it allows for a simple analysis to be made and shows a clear difference between attitudes and age groups. The statements used in this section were alarming in order to gauge the respondent’s true opinion. The presumption was that the majority of users would not be well educated in this area, as the author used statements that are not considered to be common knowledge and originated from unique sources of date.

When asking the questions in this section, an additional assumption was made that the younger generation (18-24) would have little or no opinion on the statements provided, whereas the older generation (40+) would be express themselves more, as they would not be as worried about giving a negative image of Facebook.

Analysis of Questionnaire Responses

Analysis of Respondent Demographics

This questionnaire was targeted towards Facebook users of all ages above the age of 18. In order for the questionnaire to be noticed, the author reached out to the public on different mediums, such as social networking sites, e-mails and telling people about the questionnaire through face-to-face communication. The total number of respondents that completed the questionnaire was 118. This participant count was greater than expected, with the initial aim being to surpass 75. This initial aim was set to ensure that the results would identify correlations and give a true representation of the current attitudes and awareness that the public hold towards current Facebook privacy and fabricated profiles.

As mentioned previously in the section titled "Design of Questionnaires", the questionnaire was formulated using the Google Forms service, allowing the collected results to be exported to Microsoft Excel. Excel is where the results will be analysed in depth. Of the 118 respondents, the gender had an almost even split with 56% stating they were female, and 43% stating they were male. In order to allow the user to remain completely anonymous, the author provided the option "prefer not to disclose" of which 1 respondent (<1%) chose.

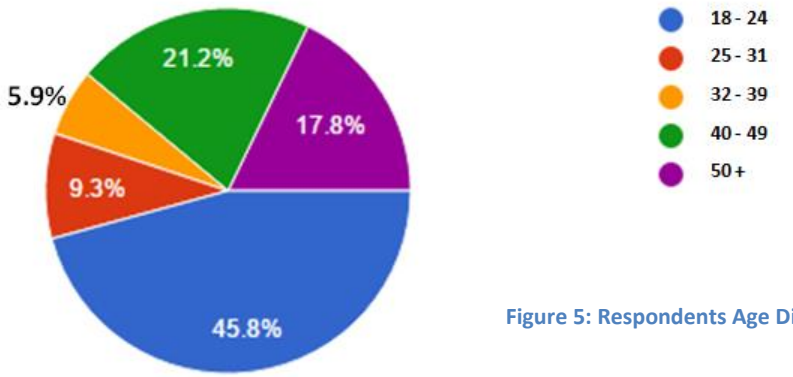

Figure 5: Respondents Age Distribution

Previously, the dangers of struggling to compare attitudes between age groups was highlighted, as the majority of respondents would be in the age range of 18-24.This assumption was formulated based on the author's social network, where the questionnaire was mainly be advertised.

Above shows the range of ages that responded to the questionnaire. There is a clear majority in favour of 18-24 year olds. When analysing the correlation between the attitudes, awareness and age, the age groups will be ranged at 18-39 (younger generation) and 40+ (older generation). Although the majority of respondents belong to the 18-39 age group, this is only a small majority of 61%. The author still feels confident that clear trends will be found and evidenced

The majority of graphical images representing the data will be presented in the form of a pie chart. This is due to the fact that the results can be clearly shown as a percentage. Due to the respondents of the questionnaire, each age group has not been equally represented. Using percentages allows the results to be proportionate to the respondents belonging to each group.

Hypotheses Testing.

The statistical method that was used to test the correlation between the users' behaviour on Facebook and the age groups was the Pearson Chi-Squared test. The Facebook experiences and behaviours have been sourced by collecting raw data which was collected from Facebook users in the form of a questionnaire and has been stored in Microsoft Excel. When analysing the results, only completed surveys were used so as to ensure the results were integral towards the overall study. As mentioned in the project methodology, the data collected represents a discrete uniform distribution. The presumption was that all outcomes would have an equal probability of occurring. This has been represented when stating the null hypothesis (**Ho**).

When Chi-Squared is used, the aim is to reject the null hypothesis stated below.
Ho: There is no correlation between age and Facebook behaviours and general security.

The formula required to complete the calculations are as follows:

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

X^2 = Chi Squared Statistic

O= Observed Frequency (Actual Response)

E= Expected Frequency (If Ho is true)

n= Number of Observations (Age Groups)

Degree of Freedom = **1**
Level of Significance = **0.10**

Analysis of respondents current Privacy and Security Awareness

The first question asked in this section (have you read through the current Facebook Privacy Terms and Conditions?) related to one of the assumptions with the aim to either prove or disprove the hypothesis. The assumption was as follows:

> **H1-** The older generation (40+) have spent more time understanding the privacy policy relating to their account compared to the younger generation of Facebook users (18-39).

The data that is used is nominal and can fall into four categories.

1. Aged 40+ and HAS read the Facebook privacy terms and conditions.
2. Aged 40+ and HAS NOT read the Facebook privacy terms and conditions.
3. Aged 18-39 and HAS read the Facebook privacy terms and conditions.
4. Aged 18-39 and HAS NOT read the Facebook privacy terms and conditions.

If the null hypothesis (**Ho**) was true - there is no difference based on age group- it would be expected in this case that the responses would be equally distributed. Shown below is the actual response in comparison to the null hypothesis.

Age Group	Yes	No	Marginal Row Totals
18-39 (Observed)	4	68	72 (61%)
Ho (Expected)	15	57	
40+ (Observed)	21	25	46 (39%)
Ho (Expected)	10	36	
No. of Respondents	25	93	118

The results were calculated showing that $\mathbf{X^2} = 27.02$, ***p***-value is .0001. This result is significant at $\mathbf{p} < .10$. This shows that there is a significant correlation between age group and the efforts made to understand Facebook's privacy terms and conditions. The null hypothesis has now been rejected. Shown below (Figure 6) is the respondents' results presented graphically in the form of a pie chart to show the clear differences in age groups.

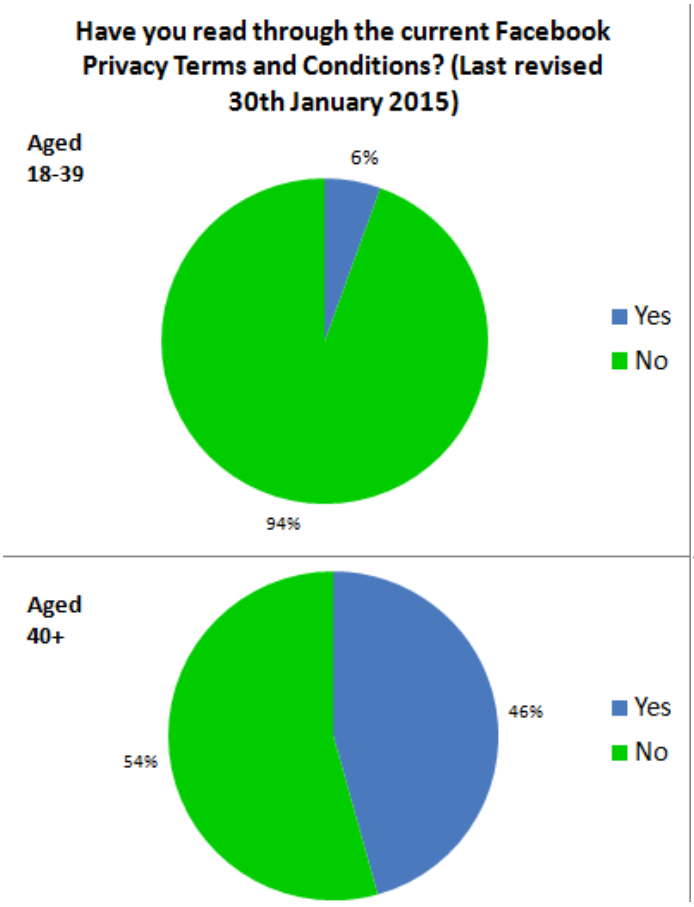

Figure 6: Graphical Representation of rejecting the null hypothesis for H1

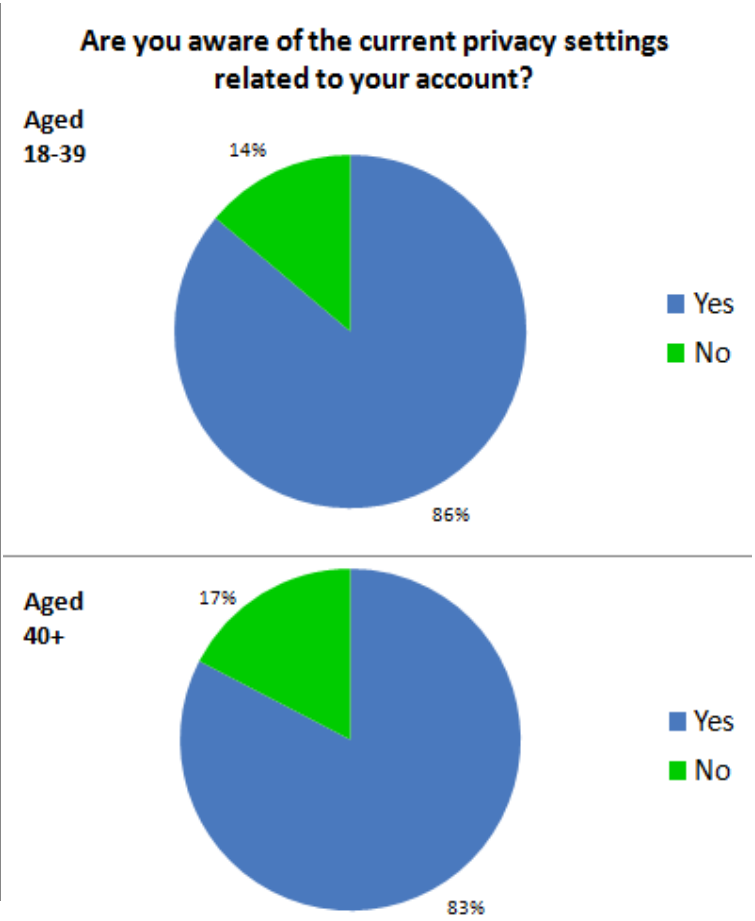

Figure 7: Awareness of the users privacy settings

The second question used in this section (are you aware of the current privacy settings related to your account?) was asked in order to measure the respondents' privacy and security awareness. This has been graphically shown above (Figure 7). The purpose of this question was to determine whether there was a difference in privacy setting awareness based on the age of the respondents using the same categories (18-39, 40+). The second hypothesis made for this section of the questionnaire is shown below.

- **H2-** Young people are ignorant with regards to privacy and over exposure on social media platforms, but are more likely to be aware of the privacy settings in relation to their account compared to the older generation.

The question only focuses on privacy settings and does not cover over exposure, meaning that the results will be able to partly prove or disprove the hypothesis with additional research being presented later. This will allow the author to determine the overall success of this assumption. When analysing the results, it became apparent that there was a similarity between the two age groups, with 14% of 18-39 year old Facebook users being unaware of their privacy settings compared to 17% of people aged over 40 using Facebook. With the difference in behaviours being minimal, the null hypothesis cannot be rejected. This means that **H2** is partly false. Further analysis will determine the overall accuracy of **H2.**

Age Group	Yes	No	Marginal Row Totals
18-39 (Observed)	62	10	72 (61%)
Ho (Expected)	61	11	
40+ (Observed)	38	8	46 (39%)
Ho (Expected)	39	7	
No. of Respondents	100	18	118

If the null hypothesis (**Ho**) were true, there would be no difference based on age group. In this case, it would be expected that the responses would be equally distributed. The results were calculated showing that $\mathbf{X^2} = 0.27$, ***p***-value is .606. This result is not significant at $\boldsymbol{p} < .10$. As a result, the null hypothesis cannot be rejected, meaning that the assumption is incorrect.

Facebook users are vulnerable to attacks by Fabricated profiles if their privacy settings are set to public. The reasoning behind this is that the fake profile will be able to access the user's content and social media footprint without raising any alarms as they gather information unknowingly. The next question, "who can view your profile content?", was asked with the intention of uncovering which age group is more likely to be attacked. Figure 8 below shows the difference in precautions taken by the users.

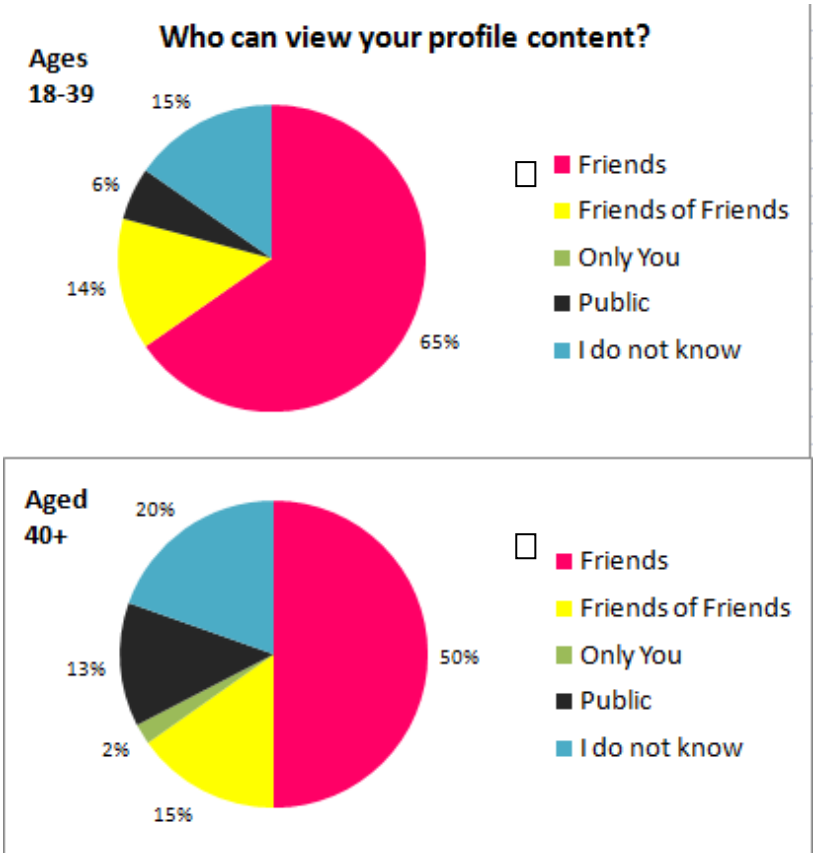

Figure 8: Who can view your profile content?

After analysing each age group, with regards to determining how accessible their profile is, both groups seem to have taken similar privacy precautions with the majority selecting to only allow "Friends" to access their social media content.

Out of the 118 respondents, 70 users (59%) chose this option. Further analysis showed that Facebook users aged 40+ are more than twice as likely to have their account set to public, with 13% of the older generation using this privacy option in comparison to only 6% of people aged between 18-39 using it. This suggests that fabricated profiles are more likely to target mature users, as there is a greater opportunity for them to access users' content due to their privacy settings.

In order to measure whether young Facebook users are more ignorant than older Facebook users in relation to social media privacy, the last question for this section was "have these questions prompted you to view your Facebook privacy settings?". The ignorance was measured by comparing the user's response to this question and a previous question, asking "are you aware of the settings relating to your account?". The response is shown below (Figure 9).

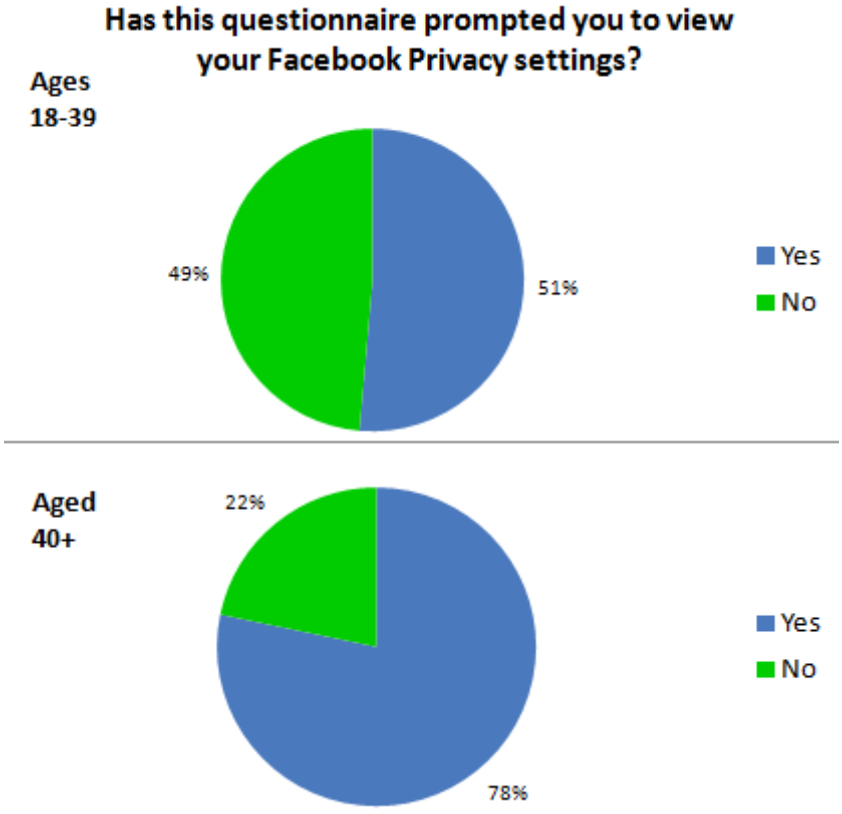

Figure 9: Measuring social media arrogance

Out of 72 respondents for Facebook users aged between 18 and 39, 35 users (49%) expressed that they did not want to view their settings. Of these 35 users, 17% previously stated that they were unaware of their settings.

Out of the 47 respondents that were aged above the age of 40, 10 users (22%) expressed a similar answer, stating that they did not want to view their settings. Of these 10 respondents, 1 user previously stated that they were unaware of their settings.

The evidence shown above suggests that there is more ignorance present in Facebook users aged below 40. After analysing both questions, it appears **H2** is partially supported with youthful Facebook users showing more ignorance with Facebook privacy, but providing no difference with awareness towards Facebook privacy settings.

Analysis of respondents' experiences with fabricated profiles.

The second section of the questionnaire had more focus on fabricated profiles. The purpose behind this section was to explore known experiences users had had with fake profiles and whether they own the credentials to a fake profile. This section allowed for both quantitative and qualitative responses throughout.

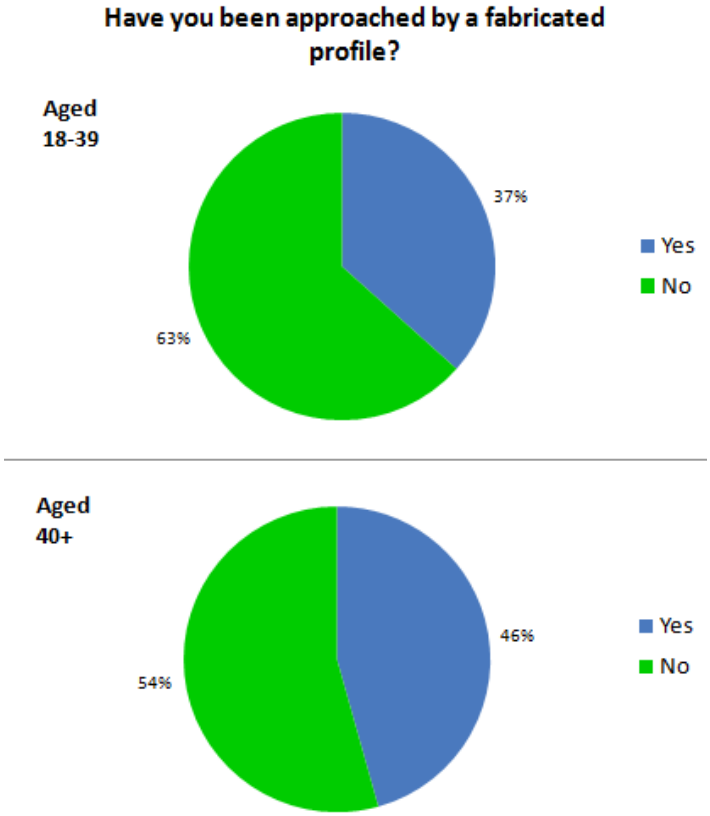

Figure 10: Respondents being approached by Fabricated Profiles

Previously, when analysing user privacy settings, it was confirmed that Facebook users above the age of 40 were more prone to having their privacy settings set to public. It is clear that there is a correlation between privacy settings and the approach of Fake profiles. Figure 10 shows that users aged over 40 are 9% more likely to have an uncomfortable experience with a fake profile. This provides evidence in favour of **H3,** proving the hypothesis to be true.

Respondents were quoted saying things such as "it was someone pretending to be an American soldier out in the Middle East. Professing his dying love for me. I blocked him after a couple of messages". Others were quoted saying "they asked for personal information such as family names.", "someone stating that they needed myself to hold money for them. Asked for my bank details" and "pretended to be customer of mine. Asking for their postal address and bank details". All of these experiences were expressed by respondents over the age of 40. As shown previously when analysing figure 10, these quotes reinforce the concept that fabricated profiles target specific age groups and users with certain privacy settings.

When analysing responses of Facebook users aged between 18-39, they seemed to prevent the fake profile from starting a conversation in the first place. These users are quoted saying "dodgy looking friend requests that I denied", " someone trying to sell things when it clearly wasn't real - hardly any friends or history on their profile.".

This shows that the younger generation hold the perception that an account is fabricated if it has little history or connection with this user. The is a misconception and can lead to more severe attacks, as the users are more likely to trust the account if mutual friends are present. This can lead to greater vulnerability.

It was stressed when creating the questionnaire that not all experiences are correct, as it is hard to define the difference between a legitimate and friendly account in comparison to a fabricated account with the intention to cause harm. This prompted an additional question, asking "what was your experience with this fake profile?". This question provided a qualitative response, and assisted when analysing the results as it aided the author in determining whether the users' experience was with a fabricated profile or not. Below (figure 11) shows a small selection of qualitative responses.

Aged 18 - 39		Aged 40+	
R1	"Fake links/scam attempts" (Spambot)	R1	"Pretending to be someone I'm already friends with"
R2	"Asking for personal information"	R2	"Threatened me to expose private information they managed to acquire"
R3	"Someone pretending to be a friend asking for information about me"	R3	"A rival company pretending to be a customer, asking for company information"
R4	"They're all the same - usually an attractive girl with a profile photo you can easily find on Google."	R4	"Someone stating that they needed someone to hold money for them. Asked for my Bank details"
R5	"Someone created a fake profile using all my friend's details and added all her friends claiming she made a new profile."	R5	"Attempted to pretend being from a company I recently bought from"

Figure 11: Qualitative Response for experiences with Fabricated profiles

In-depth analysis of respondents fabricated profile ownership.

Whilst questions were asked discovering what potential threats fabricated profiles have had towards users, additional questions were asked in order to explore the percentage of respondents owning a fake profile, and the reasons that they gave for owning one. The motivation behind this analysis occurred as a result of the author's research on Facebook's annual report, which stated that up to 11.2% of profiles are fake. This section of the questionnaire aimed to ascertain the accuracy of this statement whilst also discovering how many of these profiles were harmful towards the general public. This was uncovered by asking respondents what their motivation was behind owning the fake profile.

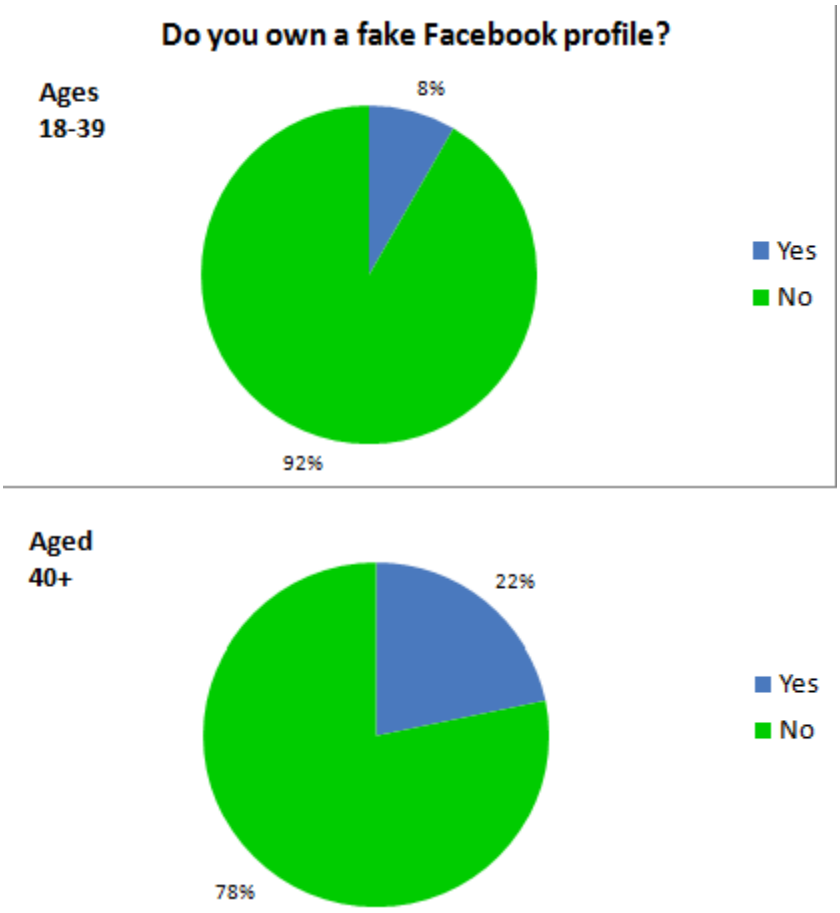

Figure 12: Respondents owning a Fabricated Profile

Figure 12 portrays the percentage of respondents owning a fabricated profile, and also shows the age group that the user falls into. Overall, 14% of respondents admitted to owning a fabricated profile, with the majority of users belonging to the 40+ age group, of which 22% answered "yes" to this question. Although the survey only accumulated 118 responses, the results appear to show that the statement released by Facebook is inaccurate, suggesting that fabricated profiles cannot be controlled and regulated.

This question also allowed the user to explain why they have a fake profile, as the question was answered in a qualitative manor. The responses were all of a similar nature, mainly related towards two categories; stalking and business. Figure 13 below shows the answers provided by the users in a table format.

Aged 18-39		Aged 40+	
R1	"To view a blocked profile"	R1	"To oversee daughters Facebook activity as my actual profile has been blocked by her"
R2	"To view a profile of someone who had blocked me"	R2	"Monitor someone doesn't say anything bad about me (ex)"
R3	"To test the visibility/security settings of me and a friends profiles after her ex was trying to make contact with her"	R3	"To stalk my Ex husband"
R4	"To only upload professional content for business"	R4	"To promote my business"
R5	"Marketing"	R5	"To try and gain a competitive edge over rival companies"
R6	"I have a fake Facebook profile to exercise my alter ego"	R6	"Wanted to test employees. Asking to disclose company information"
		R7	"Bit of fun for a couple of friends"
		R8	"To make fun of close friends"
		R9	"To send myself additional lives etc for games"
		R10	"Playing games"

Figure 13: Qualitative Response to owning a Fabricated Profile

Responses R1-R3 for both age groups relate to stalking. A study by Baum (2009) looked into victims of stalking in the United states. Over a 12 month period, it was estimated that 3.4 million people over the age of 18 were victims of stalking. Baum (2009) discovered that "approximately 1 in 4 stalking victims reported some form of cyber stalking", with 35% stating that the attack occurred via a social media service.

Stalking appeared to be the only harmful threat respondents admitted to when using a fabricated profile. The other motivations behind having a fake profile not linked to causing other users any harm related to business and personal entertainment. Responses relating to business correspond with R4 and R5 for age group 18-39, and R4- R6 for age group 40+. The response for R6 was interesting to find out, as it states that the user used a fabricated profile to test the integrity of their employees. This could be deemed as a potentially harmful incentive, as it could be harmful to the employees and there are also some ethical issues attached to this approach.

Analysis of respondents attitudes towards Facebook.

As highlighted previously, statements were presented to the respondent to gauge their understanding and knowledge on Facebook in relation to fabricated profiles. These statements were uncovered through previous research. The predicted outcome was that generally users would express anger towards the statements. Another prediction was that users aged 40+ would be more opinionated and provide personal opinions on all statements provided. There were five statements used for this questionnaire, with statements 1,2 and 5 relating to fabricated profiles, and statements 3 and 4 relating to privacy. Below are the statements that were presented to the questionnaire respondents:

Statement 1: Facebook announced in their 2013 annual report that up to 11.2% of profiles were fake

Statement 2: Of these 11.2%, it is understood that 97% say that they are Female

Statement 3: Before 2014, all new Facebook accounts were Public

Statement 4: Facebook do not inform new users of the default privacy setting

Statement 5: Facebook's current method for reducing the threat of fake profiles is to delete inactive profiles.

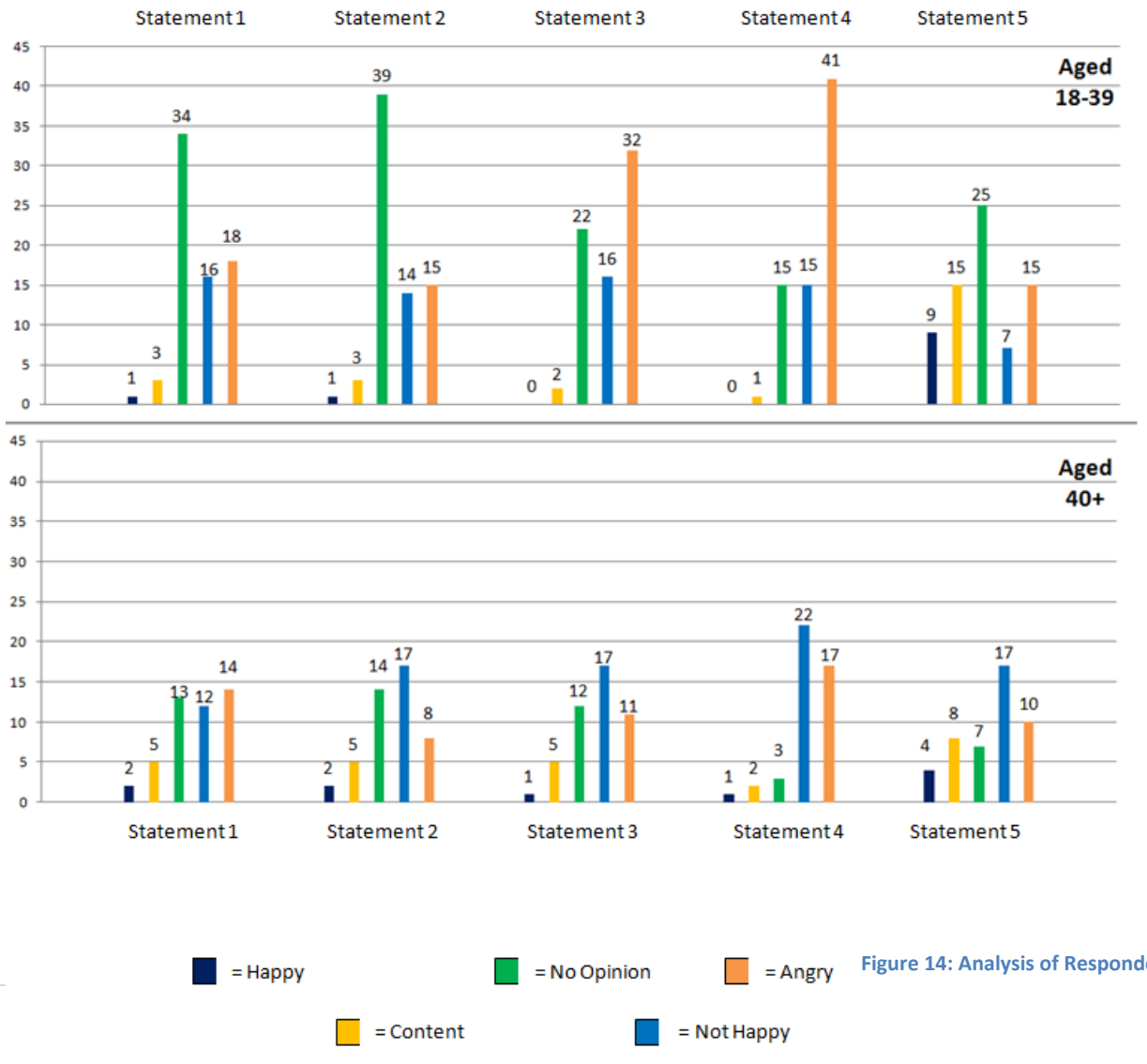

Figure 14: Analysis of Respondents Attitudes

The results presented in figure 14 show the respondents' opinions on the statements provided in the questionnaire. A key has been provided below the bar chart to show what colour corresponds to the opinion. A scale of 1-5 was provided, with 1 showing that the respondent felt happy towards the statement and 5 showing that the respondent felt angry towards the statement. When analysing this data, the combination of both "not happy" and "angry" will be interpreted as a negative response.

Firstly, statements 1 and 2 show that 47% and 54% respectively of younger Facebook users have no opinion on those statements, in comparison to just 28% and 30% respectively of the aged 40+ group providing a similar response. This would further cement the hypothesis that young users have greater ignorance towards the threat of fake profiles on social media than older users. Statement 4 had the most impact on the younger generation, with 57% of respondents stating that there were angry. This may suggest that their social media accounts contain personal information which they do not wish to share with the public. This idea will be further explored after this analysis. Overall, the results for the younger generation of Facebook users (18-39) shows that most of the statements returned a negative response. This would suggest that they were unaware of the content of the statements. Statement 5 was the only statement that returned a different reaction, with 52% stating that they were "happy" or "content" towards the current actions Facebook are taking to remove the threat of fake profiles.

Secondly, users aged 40+ expressed more opinions for all of the statements combined. Overall, older users were 17% more likely to express an opinion, either positive or negative, with 38% of users aged between 18-39 responding with "no opinion". When analysing statement 5, it was interesting to discover that there was an opposing view between the age groups, with 59% of users aged 40+ disagreeing with the younger users and providing a negative response. These results could suggest that the older generation are more aware that deleting inactive accounts is not a viable method in reducing the threat of fabricated profiles.

Questionnaire Analysis Conclusion

A number of hypotheses were tested when analysing the data gathered by the questionnaire. The questionnaire was a success, as the majority of the hypotheses were either disproved or proved, and all aims and objectives were achieved. The outcomes of the hypotheses are shown below:

H1 : A significant correlation has been discovered. There is evidence to suggest there is a relationship between age and user knowledge on Facebook privacy terms and conditions. This research shows that older Facebook users (40+) are 40% more likely to have read the terms and conditions set by Facebook.

H2 : The hypothesis has been partially proven. There is evidence for the first part of the hypothesis, suggesting that younger Facebook users show more ignorance towards Facebook privacy and over exposure. Unfortunately, this discovery does not prove the entire hypothesis, as there is evidence to suggest that there is no change in awareness towards personal Facebook privacy settings between age groups.

H3 : This hypothesis has been proven, but additional research is required in order to fully ensure that this finding is reliable and correct. The analysis from the questionnaire has found that older Facebook users are twice as likely to have their account set to 'public'. Also, older Facebook users are 10% more likely to be approached by a fabricated profile. This shows an initial correlation, providing evidence for this hypothesis.

To gain further understanding on this topic, additional questionnaires can be developed. The author of this report believes that the questionnaire that was used has been beneficial and has given a greater understanding on this area of work. Additional conclusions and reflections are provided towards the end of this report.

Facebook Risk Assessment Measure (FRAM)

Background

The risk assessment measure was used when screening started on selected questionnaire respondents. Its aim was to measure the risk of a user's profile based on the information that they have published on it. The risk was calculated based on the volume of personal information being discovered and what could occur as a result of the published information. The reason for developing this assessment was to gain further awareness on a personal level. Five subjects with different attributes and characteristics were screened to provide a variety of outcomes and to reduce the bias when conducting this study.

Hypothesis for FRAM to conclude

In order to determine whether this measurement tool is beneficial with regards to the project's methodology, hypotheses 4 and 5 were considered. These hypotheses are shown below.

- (**H4**) Social media users do not fully understand the growing risks of fake profiles and the threats that fake users can impose on innocent users.

- (**H5**) Social Media users are unaware of the information and accounts that can be accessed with the information that they have provided on their Facebook Timeline.

Objectives / Expectations

I. Be able to perform a risk assessment on any Facebook profile.

This objective was set to ensure that this assessment did not target any individuals or age groups. This precaution reduced the bias when developing results and allowed FRAM to be widely used.

II. To return a risk value to the user based on the information found.

When using FRAM, a clear end result was intended and was presented to the user. The results were categorised in the following manner:

Category	Score
Low Risk	... < ...
Medium Risk	... < ...
High Risk	... < ...
Action is Needed	... < ...

Figure 15: Categories for FRAM results

By using only 4 outcomes, the results were easier to process and communicate to the user. The score was broken down, giving personal feedback and what could be done to reduce the risk associated with their profile.

III. To provide personal feedback on each user that has been assessed.

Objectives 3 and 4 were the most important. Providing personal feedback maximised the chance of users changing their attitudes, which was the main desired outcome of the project (increasing awareness and attitudes). This was completed by showing the users what could be cultivated by using their personal details that they have provided via their Facebook account, whether this is allowing a criminal to clone their social media profile (fabricated profile), or grant access to private information stored on other online applications.

IV. To measure change (if any) in user attitudes after screening has been completed.

This was the main objective considered when developing FRAM, and was achieved by interviewing the users before and after FRAM. These interviews allowed the results to be compared, looking for changes in results. The changes were measured by the author's interpretation of the results.

V. **To understand users' social media activity by obtaining knowledge on users' content regularity and types of content that they upload. Furthermore, to conclude if users are considering threats that can occur when uploading information.**

This objective was set in order for the author to be able to analyse whether there was any correlation between social activity and vulnerability. The interviews aimed to uncover if, when user content is uploaded, the risks associated were considered. If the user states that they took prior precautions, this will demonstrate that they were aware of the current risks social media presents. As the interview was aimed at Facebook users, the author made the assumption that all of content that users uploaded was directed towards Facebook and not any of its rival social media platforms, such as Twitter and Google+.

Researching Key areas for FRAM.

In order to achieve the objectives stated above, research was required to provide an additional understanding. The key research areas have been outlined below and will contribute towards the development of the risk assessment tool.

What Defines Personal Information?

Personal data needed to be defined to ensure when screening users, the author located appropriate and relevant information for the project. The Information Commissioners Office (ICO) are an independent authority which provide an understanding towards data privacy for individuals. They suggest that personal data is "*Data which relates to a living individual who can be identified by the data in question, or other information which is in the possession of, or is likely to come in possession of the individual in question*".

This definition provided by ICO (2015) helped significantly when structuring the questions that would be asked in FRAM. Whilst discovering what personal data is, efforts were made to gain an understanding on what sensitive personal data is. The reason why efforts were made to distinguish the difference between these two was because it helped towards providing a risk value to each question. Each question would then contribute towards categorising the overall risk to a user's profiles.

Sensitive personal data as defined in section 2 of the Data Protection Act (1998) relates to the following categories:

i. His/ Her racial or ethnic origin,
ii. His/ Her political opinions,
iii. His/ Her religious beliefs or other beliefs of a similar nature,
iv. His/ Her physical or mental health or condition,
v. His/ Her criminal record.

How personal information adds risk to a social media user?

This area was explored as it contributes towards measuring the risk for each question whilst also helping FRAM to provide users with personal feedback. Furthermore, the users in question can be educated on future efforts to reduce profile vulnerabilities. Identity theft is a common threat associated with personal information. The chance of this treat occurring will be calculated by what extent personal information has been uploaded to the users profile.

ICO (2015) suggests that certain personal data entries carry greater risk towards identity theft than other kinds of personal data. They recommend extra vigilance when providing:

- Full name
- Full address
- Date of birth
- Telephone number
- School/ workplace
- Birthplace
- Previous addresses

The entries listed above will be given greater consideration when developing FRAM. If these entries have been discovered on the users social media profile, a larger risk value will be attached as it provides increased opportunities for potential criminal activity.

What types of vulnerabilities can occur once criminals acquire user's personal information?

This topic was mentioned in the related studies section of this report with a brief description of what can occur when a criminal has set up a fabricated profile using an individual's personal details. There are two main vulnerabilities; being identity theft and identity fraud.

Identity theft has been categorised into two sections; true name identity theft and account takeover identity theft. Rouse (2009) has discussed these sections and been quoted suggesting that true name identity theft is "when a thief uses personal information to open new accounts". True name identity theft has been highlighted by Rouse as a "threat which has a greater chance of occurring due to over exposure on social media". Rouse then continues to describe account takeover suggesting that it is when "the imposter uses personal information to gain access to the person's existing accounts".

Identity fraud relates closely to fabricated profiles. Once criminals retrieve a user's personal information, they are then able to commit fraudulent activity on unsuspecting targets. The aims of a fraudster is to remain hidden whilst completing the criminal act. Fabricated profiles are used to retain anonymity so the fraudster can continue to ask intrusive questions towards the target without being suspected.

Method for Screening Subjects

The analysis of a subjects Facebook account will be completed by screening their profile. Screening is when an account is investigated with all content being scanned. All content will be scrutinised against a pre defined assessment tool (FRAM). In order for screening to take place, all ethical issues listed in the project methodology will be satisfied. Most importantly, full permission had granted by all subjects involved. As the author, when screening the subjects, efforts were taken to ensure that they were aware of every action I was taking. All subjects were screened and treated independently to ensure that professionalism was consistent throughout this phase of the project. When FRAM had finalised a subject, all results were returned to the user in question. This was a necessary step to take before documentation to ensure all results were accurate and correctly represented the user.

Providing personal feedback using FRAM

In order to change the awareness and attitude of an individual, the results of FRAM will need to be analysed in depth. The sections which have been used for FRAM are defined according to the risks associated with them. By defining these, FRAM is able to highlight key areas of concern when providing feedback to the user. Whilst providing personal feedback, their score will indicate what risk boundary they relate to together with summarising results efficiently and effectively.

Section 1 - Prevalent Personal Information

Section 1 has questions relating to prevalent up to date personal information. This is the most commonly used type of information when an individual signs up for online services. Therefore this section carries the highest risk to an individual and has been weighted accordingly. Possible threats relating to this section if all questions come back positive are mainly related to Identity fraud. With online banking branching out to 70% of UK internet users in 2012 (eMarketer 2013), banks are innovating and encouraging people to open accounts online. If the entirety of this section can be acquired through your online profile, along with stating your occupation, someone is able to create a bank account in your name with various bank providers including Halifax and TSB.

Other providers including Santander, Barclays and NatWest require scanned identification, which although is possible through the criminal forging your identity, they are more likely to exploit TSB and Halifax who have relaxed constraints. Once a bank account has been made, the criminal is then able to open phone contracts and various goods and services online. This can damage your credit ratings as the contracts have been opened in your name and address.

Another attack which is related to bank accounts is the ‘SIM Swap Scam’. If the user Personal mobile number is present on their Facebook profile this attack can occur. Bank accounts can be successfully attacked where cybercriminals can divert mobile phone messages to their hand held device. This is done by the impersonator persuading the phone provider to divert mobile phone numbers, allowing them to gain security details via text message from the bank. Vahl and 'BBC You, Yours' (2016) tested this attack with worrying results. They targeted a NatWest customer, initially not knowing their bank customer number, PIN or any passwords. After diverting the customer’s mobile number, the BBC were able to change their PIN, lock the account and even transfer money out of the account.

Section 1 also relates to an individual's identity, attacks like 'Catfishing' have an increased chance of occurring if an individual's profile picture is identifiable, along with an identifiable name. A similar threat that only requires these two entities are the creation of profiles on other social media platforms. These profiles may not have the intention to seduce others, but criminals are still able to publicise content that the public can potentially be offended by and will associate this content to you which can be just as harmful.

Section 2 - Identity of Close Relatives

This section does not directly affect the risk of a user but, instead, it affects the relatives of the user. This is because the cyber criminal is able to target close relatives , opening the possibility of the attacks mentioned in this report with potentially a greater impact depending on their social media footprint.

Section 3 - Personal Attributes / Views

This sections searches for multiple views including political and religious. When sharing these views potential threats can occur as a result which include friendships and employment being affected. As social media profiles only share content to a pre-selected network of friends, users may feel comfortable sharing these views. The attitudes towards uploading this genre of content may change if a fabricated profile were to blackmail the user into sharing these views to people outside of their social network, including managers and the general public who share opposing views. This can result in the user becoming an easy target for insults and cyber bullying which can affect general confidence and self esteem.

Section 4 - Historical Personal Information

Facebook archives store uploaded users content since the creation of the account. This action by Facebook can lead to threats as users often regret the content they have uploaded or be unaware of the risks attached to the content they upload. In this section, the questions prompted include previous schools attended, previous address, and place of birth. If these come back positive suggesting the users has this information on their profile, it can significantly help criminals to map the online footprint for an individual. They can use this predefined online footprint to gain a target that is related to the user to acquire additional information for which they can use for theft or fraud.

Historical information on a user has often been used to increase the security of online accounts. The question, "previous schools attended?" is often used in security questions alongside the questions provided in section 6. By keeping content on their social media profile, it increases the chances of criminals acquiring appropriate knowledge required to answer these questions which can lead to loss of account security and increase the users vulnerabilities.

Section 5 - Professionalism of an Individual

Section 5 searches profile content that relates to a user's employment and job title. Phishing is a popular method used by cyber criminals to acquire sensitive data. This threat is focused on users who share their occupation and job title on social media. 'Whale phishing' is a digital attack targeting managers and self-employed people**.** The criminals' objective is to plant a key logger on the user's computer via the use of an E-mail. A key logger is used for surveillance and has the ability to record instant messages, E-mails and any information which is formulated from an individual's keyboard. (Spoofing) Techopedia (2016)

The criminals' main objective is to uncover confidential information which can lead to further, more substantial attacks. If a user's profile states they are a student or un-employed, criminals can still target them by altering their method of approach, changing the content of the E-mail to tailor the individual's needs.

Section 6 - Common Security Questions

'Secret' (Security) questions is a technique used by webmail platforms to authenticate account holders who are unable to login using their password. This is either because the holder has forgotten the credentials or the account has been compromised. The threats associated with the section will be focusing on E-mail accounts, using the largest webmail providers AOL, Google, Microsoft and Yahoo. The entire Facebook community are required to provide a private E-mail address through which Facebook can personally contact the account holder regarding their activity.

Questions.	Weighting	Pass/Fail	Evidence
Prevalent Personal Information			
Full Identifiable Name?	8		
Identifiable Profile Picture?	6		
Home Address?	10		
Personal mobile phone number?	8		
E-mail Address Provided?	4		
City of Residence?	4		
Date of Birth?	8		
	/48		
Identity of Close Relatives			
Parents name(s)?	8		
Siblings Name(s)?	8		
	/16		
Personal Attributes / Views			
Political View?	6		
Religious view?	6		
	/12		
Historical Personal Information			
School(s) attended?	8		
Place of Birth?	6		
Previous Address?	6		
Make of first car?	2		
	/22		
Professionalism of an Individual			
Occupation?	8		
Evidence of Breaking the Law?	8		
Actions which can potentially harm their Job security?	4		
	/20		
Common Security Questions			
What is your pet name?	2		
Where were you Born?	2		
What is your favourite Restaurant?	2		
Name of your School/ Occupation	2		
Who is your favourite singer	2		
What is your favourite town?	2		
What is your favourite Song?	2		
What is your favourite film?	2		
What is your favourite book?	2		
Where was you first job?	2		
Where did you grow up?	2		
What was your first phone number?	2		
Mothers Birthplace?	2		
Best Childhood Friend	2		
Favourite Teacher?	2		
Favourite historical person?	2		
	/32		
		TOTAL	/150

Low Risk	0 < 44
Medium Risk	45 < 89
High Risk	90 < 119
Action is Needed	120 < 150

Figure 16: Completed Measurement Tool

FRAM Focus Group Feedback

As shown in Figure 16, FRAM has now been developed. The author wanted to ensure that feedback was collected. This focus group included fellow Cardiff University students that all possessed Facebook accounts. The author provided these students with statements used for FRAM alongside the interview questions. In order to collect feedback, four questions were asked. These are set out below:

1. Are the statements suitable to reveal insecurities for a Facebook User.

2. Will the findings aid the project methodology?

3. Do the weightings for each question seem suitable in terms of adding risk to a user's online identity?

4. Are the categories well defined and explained with effective feedback being provided?

After summarising the feedback, it was clear that the focus group understood the project approach and believed the use of FRAM was an effective way to measure the change in someone's attitude and awareness towards the ongoing issue of fake profiles. After explanation, the focus group understood what each section of FRAM related to and were able to understand what threats were associated with the relevant section. As regards the question asking the focus group whether they felt the sections were correctly weighted, the group suggested weighting all security questions equally as the answer would be ultimately decided by the user and not all will be directly relevant.

Although the focus group response was mostly positive, negative feedback was received. This feedback was particularly aimed towards the first question. The focus group suggested using additional questions to create an in-depth measure covering more than just one aspect. This feedback was taken on board and prompted the author to split FRAM into various sections.

FRAM Testing

Before screening started on selected subjects, testing was required to see if the outcomes were successful. In order to test FRAM, the decision was made to use the authors own Facebook account testing the awareness before and after the risk assessment measure was used. The interview was not considered in this testing phase as the author would be able to gauge mentally if FRAM has had an impact on their social media activity. Initially, prior to screening, it should be mentioned that the author was aware of the current risks surrounding fabricated profiles as they have become educated whilst developing this measurement. Below shows the results of testing:

<table>
<tr><td colspan="3">Testing Subject: T1
Age: 21
Gender: Male
Date of Screening: 04/03/16</td></tr>
<tr><td>Initial View</td><td colspan="2">• Feels Confident that their Facebook profile will not flag threats towards the user and family.
• Expresses concerns over content that may have been published with profile creation, where user was naive and did not consider uploading sensitive information.</td></tr>
<tr><td rowspan="8"></td><td>Section</td><td>Score</td></tr>
<tr><td>Prevalent Personal Information</td><td>26/48</td></tr>
<tr><td>Identity of Close Relatives</td><td>16/16</td></tr>
<tr><td>Personal Attributes / Views</td><td>6/12</td></tr>
<tr><td>Historical Personal Information</td><td>14/22</td></tr>
<tr><td>Professionalism Of an Individual</td><td>8/20</td></tr>
<tr><td>Common Security Questions</td><td>8/32</td></tr>
<tr><td>TOTAL</td><td>78 / 150
(Medium Risk)</td></tr>
<tr><td>Post Screening View</td><td colspan="2">• Surprised by results. Did not expect that outcome.
• Will take considerable time to review profile content, deleting various uploads that have been flagged by the screening.
• Highlighted a key concern towards revealing identity of Family especially younger relatives that are still uneducated towards the risks a fabricated profile can cause towards them.
• Will now take more time before uploading content to think about potential risks it could have towards themselves and relatives.</td></tr>
</table>

Figure 17: Testing FRAM

The testing was concluded without the additional aid of the interview questions, the intended results were what was expected with the overall risk being presented to the user alongside a breakdown of the sections that were measured. The views before and after screening are shown in the table. These are additional comments the subject wishes to express before and after testing to allow in depth analysis and evaluation.

FRAM Results

Subject 1 -

Initial Interview

The interview uncovered views and activities that subject 1 participates in when using Facebook. When asking *'what is the frequency of content uploaded to your profile*?', They responded in a hesitant manor suggesting they were unaware of their activities. After thought she responded saying she "uploads photos and a status roughly once every three weeks" but stressed that she uses Facebook daily to tag 'Friends' in various articles and Facebook content that she does not own. She also said that "When uploading a statues, I often use geotagging and company names" to show where she has been and who with. When asking if she considered the risks and privacy threats associated with the content she uploads, she replied in confidence saying "No I do not", and stressed that "I rely on the security settings previously set to ensure my content is only made visible to the appropriate people.". When later asking '*Do you believe that your Facebook profile to be a potential risk towards yourself?',* She replied in a similar manor saying "No" without any hesitation. Additionally she stated that "All my network of friends I have seen in real life" suggesting she was ignorant towards the ease of duplicating profiles of close friends and acting on their behalf. The last question asking '*Do you regularly scan your social media content, deleting and altering visibility",* the response was reassuring saying "I do go back and delete content that is no longer associated with myself" saying that "old statuses were often embarrassing and not because of over exposure". After concluding the interview, the FRAM process was initiated. Below shows the results relating to the first subject screened. These results have all been confirmed by the subject after evidence was shown.

Subject: 1
Age: 21
Gender: Female
Date of Screening: 07/03/16

Initial View	• Appeared confident that her profile produced no risk towards herself in relation to over exposure. • Has made effort to keep on top of her social media footprint, by deleting old content that is no longer relevant.

Section	Score
Prevalent Personal Information	26/48
Identity of Close Relatives	16/16
Personal Attributes / Views	0/12
Historical Personal Information	16/22
Professionalism Of an Individual	16/20
Common Security Questions	16/32
TOTAL	90 / 150 (High Risk)

Post Screening View	• Mostly concerned about family members becoming under attack, as they are not efficient with technology and may not react to the attack. • Was very surprised with results returned from FRAM, after initially stating she believed there was no risks associated with her account. • Was deeply concerned that FRAM was able to uncover her breaking a law that she was unaware of.

Figure 18: FRAM Results - Subject 1

Conclusion

Prior to screening, subject 1 appeared to have little or no awareness towards fabricated profiles. The initial interview outlined that the user felt their profile had little risk of becoming a target by these fake profiles. She had this opinions due to understanding there was not sufficient content to allow cyber criminals to carry out an attack. After screening it was clear that she could be under risk with the overall score associated with her account being 90/150. The subject felt most concerned about the content on her profile showing that she had broken the law. As the author this was a surprising discovery as she frequently scanned her profile deleting content. This discovery could lead to criminals blackmailing her, threatening her career by exposing this to employees and multiple other risks that are harmful towards the user. By using FRAM on this subject it was evident throughout that her opinions and attitudes changed, with the user now understanding what threats are at high risk of occurring. The subject also understands that additional efforts are needed to reduce these threats.

As the author, FRAM had a sufficient impact on the user and shows clear reason for using this measurement for future studies and research. The process outlined what risks had most chance of occurring and abided by all the aims and objectives outlined prior to using the measurement. When holding the interview before and after the screening, it was evident that attitudes were changed. Since the screening took place the user has taken certain actions to reduce this risk, firstly by deleting evidence of breaking the law.

Subject 2

Initial Interview

Unlike subject 1, the next interview was undertaken with a subject associated with the older generation (40+). The first question asked by the author related to profile activity. The question was *'what is the frequency of content uploaded to your profile*?'. The subject responded with "I upload content very rarely, probably once a month". They answered this instantly, without hesitation. This suggested that their FRAM result would be significantly less in comparison to the other subjects'. The second question in the interview asked for '*the types of content uploaded to your profile?'.* Their response was stereotypical of the older generation, stating "only statuses, as I do not understand how to upload other content like location and photos". When responding to this question, the subject appeared to be embarrassed by sharing this honest answer with the author. This potentially shows a lack of confidence when using social media platforms, further suggesting that their profile content was limited in comparison to the other subjects. Although the subject appeared to be uneducated with regards to Facebook, they did consider the privacy of their account. When asked '*do you consider the risks associated with the content you upload?',* they responded with "Occasionally, depending on the material being uploaded". This response made the author more confident that the user would produce a low score, as they assess the potential risks associated with each upload. Following on from this question, even though the user did not know all of their "Facebook friends" personally in a real world environment, it was of little surprise that subject two felt that their account was at very little risk with regards to over exposure. However, due to the fact that subject 2 has friends on Facebook that they do not know, their chances of having a fabricated profile already attached to their social media profile have increased. This concluded the interview and prompted FRAM to start. After the evidence was shared with the subject, they confirmed all of the results.

Testing Subject: S2
Age: 49
Gender: Male
Date of Screening: 09/03/16

Initial View

- Was confident throughout interview, and felt their profile would not contribute to the threat of cyber attacks.
- Has made prior effort to consider risks before uploading content. This should have a direct effort on the overall score.

Section	Score
Prevalent Personal Information	12/48
Identity of Close Relatives	8/16
Personal Attributes / Views	12/12
Historical Personal Information	6/22
Professionalism Of an Individual	4/20
Common Security Questions	6/32
TOTAL	48 / 150 (Medium Risk)

Post Screening View

- Although FRAM suggested his account was medium risk, little actions will be taken as a direct result of partaking in FRAM.
- His score is reflected on the lower side of the risk boundary (Medium). After informing the subject of the risks associated with personal views (highest scoring section), the user will give greater thought before publishing more content relating to this section.
- No other sections were raised as an immediate concern. The user is satisfied with the overall FRAM result.

Figure 19: FRAM Results - Subject 2

Conclusion

On completion of subject 2's FRAM profile screening procedure, the subject's personal attitudes and views did not seem to change. When screening the profile, an alias and a non-identifiable profile picture were used to cover the subject's real identity. These were steps taken by the user to reduce their social network footprint. The results revealed that this precaution worked, as section 1, prevalent personal information, only scored 12/48. The only section to raise any concerns for the subject related to personal views and attributes. The maximum amount of marks were received by the user in this section. Although the risks relating to this section appeared to have no affect on the user's attitudes, the user was unaware that this information was openly available on their social media account and the user has since taken the appropriate actions to delete this content from their page.

In conclusion, there was not a sufficient impact on the subject as a result of FRAM. This was not consistent with the initial projections made when developing the measurement tool. Although the impact was not substantial, the user has still taken additional actions to delete content which would otherwise have continued to be widely accessible. This action still justifies FRAM being a viable tool for increasing social media user awareness.

Subject 3

Initial Interview

Subject 3, unlike previous subjects, uses Facebook for both personal and professional use by advertising business activities and events on their 'Timeline'. By using Facebook for publicising their business alongside their personal content, it was expected that greater amounts of information would be openly available and increase the chances of over exposure. When asked '*what is the frequency of content uploaded to their profile*?' their response was reassuring, as they stated "I upload statuses on a daily basis relating to both business and personal content. But I rarely post events and photos". This suggested that they use other online services for these tasks. This was the only confident response throughout the interview and the following questions required greater thought. Although the subject was expected to have sensitive information on their Facebook profile, it was interesting to discover that little effort was taken to consider the risks associated with the content that they uploaded. The subjected was quoted saying "I never do, and trust my security settings to ensure my content is safe and only visible to my 'friends'." Although they never considered the risks, they appeared to be aware of the fact that their profile could be a potential risk towards them-self. Their response to this was "Yes, If presented to someone with the wrong intentions". This showed that prior to screening, they were aware of the risks surrounding fabricated profiles and over exposure. When asked what these risks could be, they replied with "Blackmail, and I suppose someone could create a fake profile on me as all my information is present on my profile". The user also stated that they had not spoken to all of their 'friends' in real life, stating that "some are friends of friends". This concluded the interview and prompted FRAM to start. All results were confirmed by the subject after evidence was shared with them.

Testing Subject: S3
Age: 32
Gender: Female
Date of Screening: 13/03/16

Initial View	• User has never considered the risks when uploading content, but confessed that her profile could potentially be a threat towards herself if accessed by the wrong people. • Although the subject has deleted old profile content, this action has taken to avoid embarrassment and not over exposure.

Section	Score
Prevalent Personal Information	48/48
Identity of Close Relatives	8/16
Personal Attributes / Views	12/12
Historical Personal Information	14/22
Professionalism Of an Individual	8/20
Common Security Questions	12/32
TOTAL	102 / 150 (High Risk)

Post Screening View	• Informed the user that she was the highest scoring subject out of the five that were screened. She was shocked by this. • The subject has also scored maximum marks for 'Prevalent Personal information' which is associated with the most threatening risks. • • She believe that using her account for both personal and business has had a large, negative impact on the result.

Figure 20: FRAM Results - Subject 3

Conclusion

Subject 3 was the only subject to use their Facebook account for both professional and personal use, which as a result was reflected in the outcome of the FRAM. Although the user stated that they were aware that their profile was potentially a risk towards them-self, they were left surprised when the additional risks that was previously unknown to them were shared. The user accepted that an in-depth fabricated profile could be generated based on their uploaded content, but was completely unaware of the threats relating to their company and bank account. Section 5, on security questions, scored 12/32. This was not considered to be a high enough score to say that the user was at high risk. Although this section scored fairly low, the user was extremely surprised. Due to the subject's reaction, it was clear that the answers given to subject by the author were the correct answers to their current security questions. This breakthrough was regarding confidential information and the user was not happy disclosing it. However, they did express that they would take the time to delete this information off of their social media profile.

FRAM had a clear an impact on the subject, their awareness of the subject of this study was changed and improved. These results prompted the user to think about their future use of social media. It was recommended by the author that the subject should create separate accounts for personal and professional activities, with their business account being un-identifiable to the owner. Although this subject made prior precautions to reduce their social media exposure, it was clear after concluding their results that they are not correctly educated around this topic and further work is needed.

Subject 4

Initial Interview

Subject 4 represented the 18-39 age group, at the age of 21. When delivering the interview questions to the subject, they appeared indifferent throughout the interview. This view was based on their responses and facial expressions. When discussing their Facebook activity, asking '*how often do you upload content to Facebook?',* the subject replied “once every two months roughly". It would appear that this subject uses Facebook the least when compared to the other subjects that were screened, suggesting that the subject would have the least amount of content available to view. This was represented in the outcome of FRAM. Although the subject uploads small amounts of content, they appear to still consider the risks of each status, stating "yes” when asked. This response was reflected in the following questions, as the subject seemed to believe that their profile did not cause a potential risk towards them-self, even though they confessed that they make no effort to regularly scan old social media content to adjust its visibility. The last question asked whether the user has communicated with all of their 'friends' outside of Facebook. They responded with "no". This reply raised immediate concerns, as fake users could already be connected to their social media network. All of the questions were completed in a professional manor, and all of the results returned by FRAM were confirmed by the subject after evidence was presented to them.

Testing Subject: S4
Age: 21
Gender: Male
Date of Screening: 15/03/16

Initial View	• Although risks were considered, subject seemed arrogant towards the study. • User was indifferent throughout the interview, was confident that FRAM will return no risks or sensitive information. • The subject has the least Facebook activity out of all subjects being screened.	
[redacted]	**Section**	**Score**
	Prevalent Personal Information	44/48
	Identity of Close Relatives	16/16
	Personal Attributes / Views	0/12
	Historical Personal Information	8/22
	Professionalism Of an Individual	12/20
	Common Security Questions	14/32
	TOTAL	94 / 150 (High Risk)
Post Screening View	• Was unaware that home address was visible. Although split amongst two separate statuses (One including house number, other providing the street name) • User was initially unaware of the evidence being presented to them. Was in denial throughout. • Although section 1, and 2 scored highest, the users was most concerned with the security questions. Upon showing evidence, user confessed to using answers provided on their social media.	

Figure 21: FRAM Results - Subject 4

Conclusion

Subject 4 appeared to be ignorant throughout the interview. Upon deeper analysis, this subject answered the interview questions with similar answers to the ones they gave for the questionnaire, responding in a manner that aided towards confirming one of the hypotheses. When presented with the results, the user's views and attitudes did not appear to change, even though their results were alarming. The user seemed surprised with the amount of information that the author was able to collect on the individual, but stated that this would not change their future activity on social media. If a fabricated user was to target this account, the threat of hacking the e-mail address associated with this account was possible, with the user confessing that one of the security questions was openly viewable on their social media account. When similar results were discussed with the other subjects being used for the study, their attitudes and views changed and impacted their future social media use. The author of this project believes that this is not the case with subject 4 due to the ignorance they displayed with regards to their privacy.

To conclude, FRAM produced sufficient results. It is expected that these results would impact the majority of social media users. Youthful ignorance towards this topic was clearly shown with this subject and impacted the overall outcome.

Subject 5

Initial Interview

Subject 5 was the last user screened and concluded the FRAM process. When asked '*how often do you upload content to Facebook?*', the subject replied in a very slow manor, clearly thinking about their answer carefully, stating "once a week, often when I'm doing something with family and friends.". When interpreting this answer, it was presumed that section 2,'identity of close relatives', would score highly because of this response. The subject also responded to '*do you consider the risk associated with the content you upload?*' in a similar manor, stating "never, I do not usually think about that. I probably should though". When responding to this question, the subject's facial expression appeared concerned that FRAM could potentially produce disconcerting results. This response was also replicated later in the interview when asked '*do you regularly scan your social media content?'.* Before asking the following question, '*do you consider your profile to be a potential risk towards yourself',* from interpreting previous answers it was expected that the subject's response would suggest that their profile was at risk. Their actual response was not what was expected, as they stated "no big risk, or risks that could be aimed at me directly." The last question of the interview asked the subject whether that have communicated with all of their 'friends' outside of Facebook. The subject responded in a confident tone, stating" no, usually just accept all incoming friend requests". This answer displayed some ignorance towards the issue of fabricated profiles. After the FRAM screening process was completed, all of the results were confirmed by the subject after evidence was presented to them.

Subject: S5 **Age:** 27 **Gender:** Male **Date of Screening:** 18/03/16		
Initial View	• Hesitated throughout the Interview, was unsure on many responses. • The subject was confident that their profile would return no substantial risks. • The only subject to admit to accepting any friend request.	
[redacted]	**Section**	**Score**
	Prevalent Personal Information	26/48
	Identity of Close Relatives	16/16
	Personal Attributes / Views	0/12
	Historical Personal Information	16/22
	Professionalism Of an Individual	16/20
	Common Security Questions	16/32
	TOTAL	80 / 150 (Medium Risk)
Post Screening View	• Had little reaction to the results, appeared not to care towards the potential risks possible due to the content on their Facebook profile. • Section 2 information was all available. This was expected by the author before screening started. • Users awareness has not changed, with the subject not changing any actions or views as a result of FRAM.	

Figure 22: FRAM Results - Subject 5

Conclusion

Subject 5 was one of the two users that did not change awareness and attitudes significantly as a result of the FRAM process. The subject was hesitant throughout the interview, potentially realising that they should have more precautions in place to prevent over exposure online. This hesitancy was noticeable when the subject admitted to accepting all incoming friend requests with no method in place to filter legitimate and fake accounts. This subject was the only Facebook user to possess this methodology. Although limited research had gone into the risks surrounding this procedure, earlier analysis provided by the questionnaire suggested that there was a strong possibility that people were using fabricated accounts to stalk this subject without the user being aware. When presenting results to the user, little care was shown even though their profile appeared to show him breaking the law. This could potentially affect their career, and this was also stated to them. This aided in confirming previous assumptions that suggested that younger social media users have little awareness towards the growing concern surrounding fabricated profiles, and the damage that they can achieve by simply screening a Facebook profile.
This subject did not represent the overall FRAM process, with the majority of users showing great concern and sharing their intent to change the way they use social media and the content that they upload with the author. Following this analysis, the following section will continue to conclude the FRAM process by drawing overall conclusions and discusses whether FRAM is a viable process with regards to raising Facebook users' awareness on over exposure and fabricated profiles.

FRAM Analysis

This section will now discuss the effectiveness of FRAM. Prior to the development of this tool, aims and objectives were set to aid in concluding the success of FRAM, and how beneficial it was towards this project's methodology. These aims are outlined below:

1) Be able to perform a risk assessment on any Facebook profile.
2) To provide personalised feedback on each user being assessed.
3) To return a risk value to the user based on the information found.
4) To measure change (if any) in user attitude after screening has been completed.

The author's decision on whether FRAM succeeded in achieving these aims was based on an interpretation of each of the individuals' outcomes. The author also ensured that ethical statements 7,8 and 9 were followed correctly. These statements can be found in the section titled 'Project Planning and Methodology".

Firstly, when screening the five subjects, efforts were made to ensure that the subjects had various unique attributes. These attribute consisted of age, gender, social media activity, prior knowledge, and precautions taken. This outlined whether the assessment could be undertaken on any individual owning a social media account. As results were produced for all of the subjects, it is clear that FRAM was able to perform a risk assessment on any Facebook user, therefore achieving the first objective.

The results that were shared with the user consisted of various sections and presented a personal score unique to each subject. In addition to this, the author explained any threats associated with their social media account to the subject. By breaking down the score, the author was able to locate the section that produced the highest score and therefore could provide appropriate feedback to the user and explain the potential attacks relating to their profile. These steps arguably satisfy aims 2 and 3.

Aim 4 was also successfully achieved. This was due the fact that an interview was conducted before and after the subjects' profiles were screened. As previously mentioned, the interviews allowed the author to analyse any changes in the subjects' attitudes, enabling him to consider factors such as their facial expressions and tone of voice. These also aided the author in deciding whether FRAM had a direct impact on the users' behaviours or not. It is clear that all of the aims and objectives were achieved.

In addition to discussing the aims and objectives, this section also allowed the author to assess the results and data produced by FRAM. When comparing all of the interview answers before and after the screening took place, it seems that all of the subjects enhanced their knowledge and awareness on the topic of this project.

The main purpose of this part of the project was to educate users on this area and to encourage them to take action in preventing their own victimisation. Three of the subjects confirmed that they intended to take action in order to remove harmful content from their profiles. The subjects were made aware of this harmful content during the screening process. The other 2 subjects, although confirming that they did not intend to take any action, did aid in proving the hypothesis regarding the ignorance of the younger generation to be correct with regards to this project. It was also discovered that only 1 of the subjects took precautions prior to their FRAM report. This was highlighted in the outcome of that subject's screening, as they scored the lowest score of all of the subjects. That particular subject created an alias and an alternative profile picture, therefore disregarding Facebook's current terms and conditions and meaning that their profile is considered to be fake. This highlights the fact that all Facebook users are at risk by simply abiding to the current policy, due to the fact that they must provide an identifiable name and picture, among other things.

Future Work

Although there is very limited research currently surrounding the topic of fabricated profiles, the author was still able to produce results of a good quality and standard. Despite this, the project did have some limitations, one of these being a time constraint. The time limit affected the project more than was originally intended, and as a result, some of the additional work needed to support the study further was not completed. Although this appears to be a slight setback, it does allow for the study to be further enhanced and developed.

FRAM has proven to be an effective way of investigating user awareness towards the risk of fabricated profiles, and in educating users on their social media behaviours that can potentially increase the chance of them becoming a victim. FRAM is also capable of analysing users' change in attitudes towards this subject by conducting interviews before and after screening. One drawback pf FRAM is the amount of resources that are required in order to screen users. The entire FRAM process is non-automated. This means that the author has to manually filter through the user's Facebook content and flag up any information that presents a risk to the user. The first idea for future work would be to automate the process and develop a program to support the screening process. As the author of this project owns the risk assessment measure, simplified wireframes were able to be developed in order to portray the author's vision. These wireframes were created using Visual Paradigm and are shown below:

Figure 23: Wireframe 1

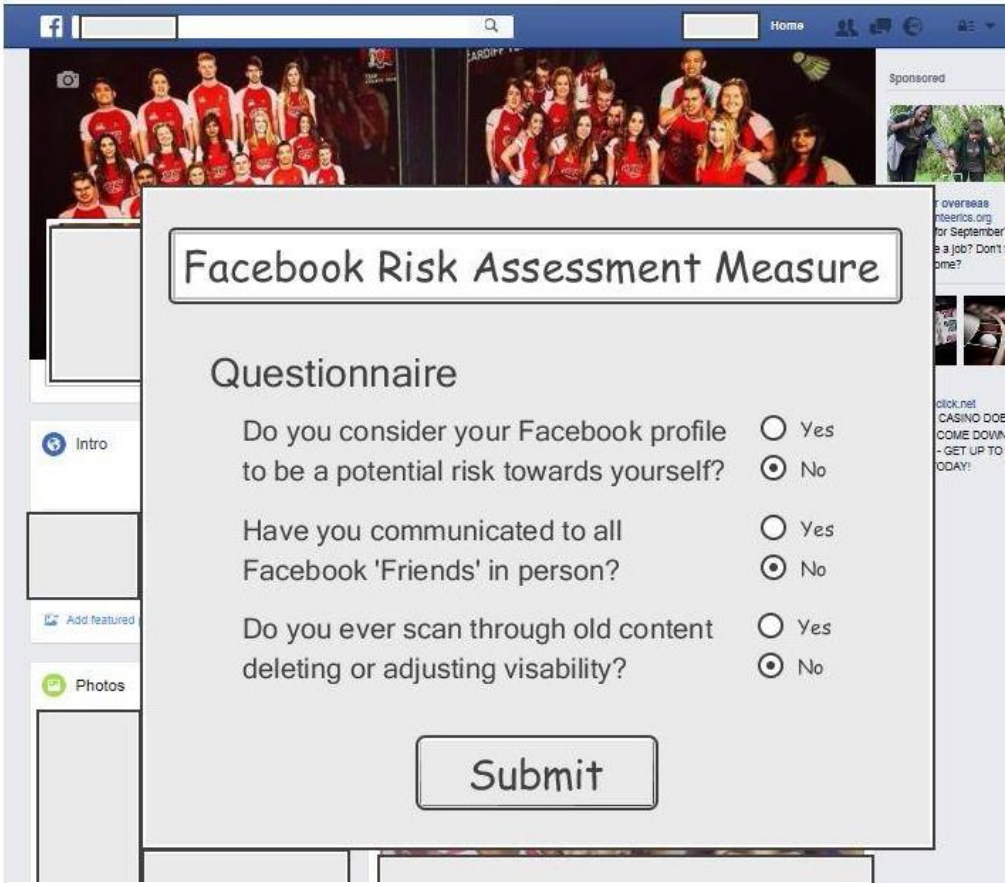

Figure 24: Wireframe 2

Figure 25: Wireframe 3

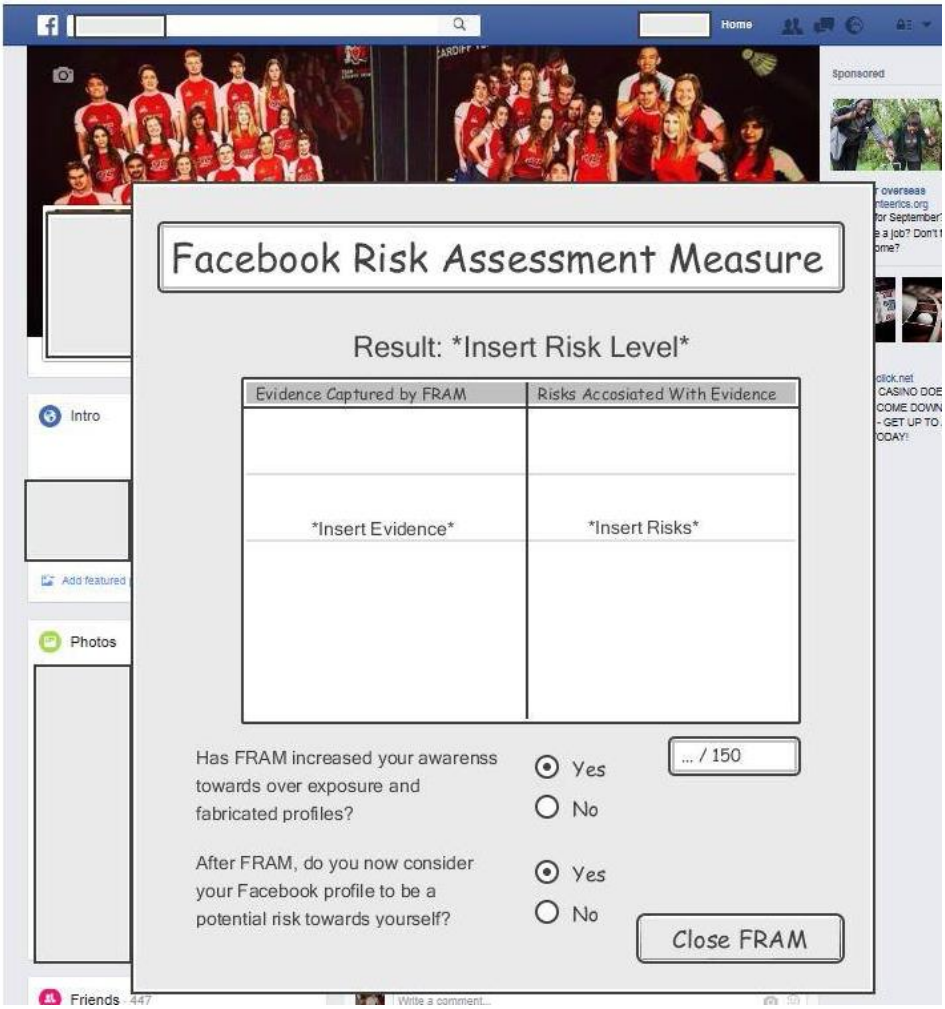

Figure 26: Wireframe 4

If FRAM was automated, a greater number of social media users could be screened, as the time taken to screen the users would be significantly reduced. As only five subjects were screened for this project, the conclusions and analysis could be interpreted by some as inaccurate due to the fact that the results were not calculated from a large sample of social media users. The proposal to automate FRAM could resolve this issue by supporting the study and ensuring that the results produced were accurate.

Additional future work can be completed to further support this project. During the project, some additional work was considered but time limitations prevented the author from completing this work. Instead, greater effort was spent ensuring that key deliverables were completed. This additional work has been outlined below:

- To develop and carry out further research using FRAM using a larger sample size to create proven, accurate data.

- Develop a greater understanding on fabricated profile threats and attacks on innocent social media users.

- Develop an additional questionnaire to further explore awareness and attitudes social media users have towards fabricated profiles. Unlike the current project path, specific attitudes should be focused on to create unique research outcomes.

- When developing additional research methods, the sampling size should be increased with greater efforts to ensure all age groups analysed are equally represented. The current sampling size and demographic is a limitation towards research outcomes.

- When analysing future research, a greater age demographic is to be used. Currently 18-39 and 40+ are in use, with clear changes in attitudes and awareness being presented. The current demographic does not accurately define which ages show passive behaviours and which takeprecautions towards fabricated profiles.

- Develop prototypes that increase awareness towards what profile content adds risk towards an individual.

- To bring prototypes developed from this project forward to social media developers, to ensure resources are used to implement systems to prevent the creation of fabricated profiles, whilst also increasing awareness towards threats associated with fabricated profiles to Facebook users that have not been reached by this study.

- Implement research on other social media platforms regarding this area of work. Compare social media sites to outline which platforms expose sensitive data the most (user activity)

Changed Deliverables

It was stated in the initial project plan that work would be completed on developing controls that could be implemented by Facebook to increase the awareness of fabricated profiles. When these plans were proposed to the project supervisor, it was recommended by them that the author focus on delivering accurate, well thought out research whilst also creating an effective risk measurement tool that would support the methodology of this project.

Conclusions

In conclusion, this project has created the necessary steps towards investigating the awareness that users have to the risk of fabricated profiles, whilstalso recommending approaches in educating users on the prevention of becoming a victim. The education of users on this matter was an underlying aim throughout the project, one that I believe has been satisfied. While FRAM was used to educate social media users for this project, there are other ways of further supporting this project and expanding social media users' knowledge on the subject. These ideas have been outlined in the 'future work' section of the report.

The project also had the intention of proving or disproving assumptions that were created at the beginning of the study. I believe that the majority of these assumptions were tested and produced a satisfying outcome. In spite of these outcomes, I do feel that additional work is needed in order to ensure that all of the areas of this topic have been researched and evidenced. I also feel that, as there is currently very limited research on fabricated profiles, this project has made a good headway in the area. This is due to the fact that the primary research conducted as part of this study has produced decisive results and statistics that truly represent the current attitudes owned by social media users on this topic. Although this project as a whole has been mostly positive, there are some areas in which improvements could be made. Although FRAM produced very promising results, due to the time limitation on the project, I was only able to screen five social media users. This, therefore, did not produce results that were decisive enough to prove certain hypotheses to be correct. Furthermore, they were not as helpful in supporting the overall effectiveness of the project as they could have been. The necessary steps required to solve this problem are outlined in the 'future work' section of the project. Despite this minor setback, I still feel very positive and optimistic with the direction that this project has taken.

I have ensured that this project has been well documented, providing justifications and analysis throughout. I believe that these efforts have aided in promoting the threats caused by fabricated profiles, whilst also aiding in the impact on social media users' attitudes and awareness. These aims have been satisfied due to the completion of the following tasks:

- In-depth documentation on previous research relating to this study, all of which have contributed towards my project aims and outcomes.

- A well detailed, thought out questionnaire designed to understand attitudes among various age groups.

- In-depth analysis of raw data collected by the questionnaire, using statistical measurements which have been used to aid in proving or disproving pre-defined hypothesis.

- The creation of a measurement tool used to educate social media users on over exposure and risks associated with the content that they upload.

Reflection on Project

This section will focus on my reflection on the project and will discuss what I have learnt whilst developing it from start to finish. From the beginning of this project, I understood the level of work and effort that was required to deliver a project in this area of work. As the project was proposed by myself, I had an initial understanding of the direction it would take and the final deliverables that were required to complete it. However, at the start I mistakenly considered this report to be one large piece of coursework rather than a collection of small, manageable segments. I believe that I was initially quite naïve, however this project has taught me the importance of breaking down a large piece of work into smaller and manageable sections in order to ensure optimum quality is reached throughout. Nonetheless, I feel I still delivered a high standard of work throughout this project. In the early stages of this paper, I found it difficult to prioritise and balance my focus between writing the report and researching it. When completing the 'related studies' section, which looked through previous research projects, I gained a helpful insight into what was expected of me and acquired a clearer picture of what my deliverables should look like and contain, particularly with regards to the questionnaire. This sectioned outlined the importance of research to me.

On completion of this project, I became aware that the outcome of the investigation on fabricated profiles was not what I intended it to be. Originally, I intended to investigate the motivations behind fabricated profiles in general. However, the project's focus shifted towards exploring users' awareness and attitudes towards fabricated profiles, and the difference in experiences of them depending on the age group. This change in direction is reflected in the hypotheses throughout the project. On reflection, I believe this change occurred because I was not exactly sure what I wanted to achieve from the project, and my interests in the outcome changed. I became more interested in how experiences of fake profiles differed depending on age as opposed to what people use those fake profiles for. As a result of this change, I believe that the biggest lesson I have learnt from this project is that with any future project, the intended objectives and outcomes must be clearly outlined at the start, so that the project deliverables at the end are what they were expected to be at the start.

With the questionnaire being the main research focus, I wanted to ensure that sufficient time and effort was spent on this section. Before I started this project, I did not put much effort into creating questionnaires and did not think about their layout or their content in great depth. This process has taught me the importance of planning the questionnaire effectively, ensuring that it has the ability to produce worthwhile results that are of the highest standard. This efficient planning has ensured that my research results surpassed any secondary sources available to me. The outcomes of this questionnaire were influential to my final project and I feel that the aims and objectives were surpassed. However, with my project consisting entirely of research, I feel opportunities were missed when the questionnaire was released. In hindsight, more questions should have been used to cover various other topics which would have given greater depth when analysing and testing various other hypotheses. This action would have helped towards the final project and the conclusions that were derived from the research. I now know that with any future research,

every effort should be made to ensure that all areas of the project are covered in order for effective outcomes to be formulate. This can be achieved by spending more time and effort on defining the purpose of the questionnaire, and spending more time on background research for the areas I wish to analyse. I also feel that respondents' demographics affected analysis more than expected. When finalising the project methodology, it was outlined that respondents may be biased as this questionnaire was mainly advertised through my social media network. With analysis focusing on differences of attitudes between age groups, more effort should have been made to ensure that these age groups were equally represented.

Although this complication was expected, it has had a more negative affect than originally intended. This complication has taught me to give more thought towards demographics and the importance it can have when analysing results. This lesson will be brought forward to any future projects I partake in. However, I still feel that my questionnaire was successful with the response rate being overwhelming and surpassing my original expectations. Therefore, I feel that the conclusions derived from the questionnaire are still relatively accurate and reliable, and that the questionnaire produced sufficient outcomes.

Before the project began, an initial plan was required to aid in outlining the expectations and deliverables. An appropriate timescale was created to ensure that all work was completed on time. Although I feel that the timescale was appropriate for this project alone, external factors were not considered when creating it. The only factors considered were educational ones and related to additional modules I was taking alongside this project. Although these factors were considered when creating the timescale, personal factors were not. This planning error affected the project throughout. In hindsight, I should have considered this further, as I did not allow myself enough time to complete work from other modules in this time scale. When partaking in any future projects, I will consider all of these factors in greater depth in order to ensure that the project runs smoothly.

Once the project was initiated, background research was undertaken. As mentioned previously, this project was proposed by myself as I feel passionate on the subject and felt awareness needed improving on this specific social media threat. With any research project, related studies influence the direction of the project and contribute significantly. I feel I was unable to use this to its full potential. I was confident before starting, that adequate research had already been undergone in this area of work. This was a misconception, and little research was available to use which was relevant to my study. This caused time to be wasted as greater efforts were needed to find relevant studies. This time could have been spent in other areas which would have had greater impact on my project. This problem was a steep learning curve and lessons have been learnt as result. With future studies, I need to research the topic before taking the task on. This step will prevent this issue from occurring again.

Once primary research was analysed, the next phase of the project was to develop a risk measurement tool. This phase of the project was intended to increase awareness of this growing threat on social media. As previously stated in the 'future work' section, the development process took longer than intended and therefore affected the deployment of the tool. Subsequently, I could only use the tool on five subjects. I believe that more thought should have gone into this phase, and I could have potentially changed the approach and method used. In hindsight, an automated system could have been created. This process may have taken longer to implement, but deployment time would have been reduced, therefore screening could have taken place on more subjects.

Lastly, my questionnaire analysis and FRAM were connected and explored the same area of work. On reflection, this connection was not profound enough and has resulted in the project appearing to be split into two separate studies. In hindsight, I should have made better plans to link the two together, making my overall project more complete.

Overall, I feel that this project and module has given me valuable experience on how to effectively tackle and execute future projects of this magnitude. With this project being independent and consisting of my own work, I feel that I have become a stronger independent worker as a result. Prior to this project, I would have considered myself to be stronger in a group environment, however this project has changed my opinion. I have made sure all aspects of the project were completed on time and met deadlines which were set in the time plan shown in the initial report. I am confident with the work that I have produced and I believe this report justifies my confidence.

References

The Guardian (2016) Available at: http://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers (Accessed: 21 February 2016).

Statista (2015) Facebook - Statistics & Facts. Available at: http://www.statista.com/topics/751/facebook/ (Accessed: 17 February 2016).

Facebook (2013) Facebook - Annual Report. Available at: http://investor.fb.com/secfiling.cfm?filingid=1326801-14-7&CIK=1326801 (Accessed: 22 February 2016).

Liu, Y. (2011) Analyzing Facebook Privacy Settings. Available at: http://dl.acm.org/citation.cfm?id=2068823 (Accessed: 22 February 2016).

Magid, L. (2014) Facebook changes new user default privacy setting to friends only -- adds privacy checkup. Available at: http://www.forbes.com/sites/larrymagid/2014/05/22/facebook-changes-default-privacy-setting-for-new-users/#70adbef3725f (Accessed: 26 February 2016).

PPR (2015) The Evolution of Facebook's Privacy Policy. Available at: http://techscience.org/a/2015081102/ (Accessed: 24 February 2016).

Krombholz, K. (2012) 'Fake Identities in Social Media: A case study on the sustainability of the Facebook business model', Journal of Service Science Research, pp. 175–212.

Barracuda Networks (2012) How to Identify Fake Facebook Accounts. Available at: http://www.cnet.com/how-to/how-to-identify-fake-facebook-accounts/ (Accessed: 22 February 2016).

Lavasoft (2013) Are we Overexposing Ourselves on Social Networks? Available at: http://www.lavasoft.com/mylavasoft/company/blog/are-we-overexposing-ourselves-on-social-networks (Accessed: 24 February 2016).

Abine (2013) Social Media Footprints. Available at: https://www.abine.com/about/press-releases/ (Accessed: 25 February 2016).

Ghazinour, K. (2013) Monitoring and Recommending Privacy Settings in Social Networks. Available at: http://www.mathcs.emory.edu/pais13/pdf/PAIS2013_Paper7.pdf (Accessed: 27 February 2016).

Sophos (2007) Study: Facebook users easy targets for identity theft. Available at: http://www.macworld.com/article/1059488/facebook.html (Accessed: 28 February 2016).

Bryman, A. and Bell, E. (2011) Business Research Methods. Third Edition .Oxford University Press, pp 57-58.

Cambridge Dictionaries (2016) Fake Meaning. Available at: http://dictionary.cambridge.org/dictionary/english/fake (Accessed: 29 February 2016).

Facebook (2016) Terms of service. Available at: https://www.facebook.com/legal/terms (Accessed: 1 March 2016).

Facebook (2016) Data policy. Available at: https://www.facebook.com/about/privacy/ (Accessed: 1 March 2016).

Griffin, A. (2015) Facebook to tweak 'real name' policy after backlash from LGBT groups and native Americans. Available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-to-tweak-real-name-policy-after-backlash-from-lgbt-groups-and-native-americans-a6717061.html (Accessed: 02 March 2016).

Hampton (2011) Social networking sites and our lives. Available at: http://www.pewinternet.org/files/old-media//Files/Reports/2011/PIP%20-%20Social%20networking%20sites%20and%20our%20lives.pdf (Accessed: 3 March 2016).

Gallagher, B. (2013) 10 ways to tell if your new Facebook friend is a Spam Bot - 10. She wants to show you her Webcam. Available at: http://uk.complex.com/pop-culture/2013/08/facebook-spam-bot/she-wants-to-show-you-her-web-cam (Accessed: 4 March 2016).

Battersby, L. (2015) Millions of social media photos found on child exploitation sharing sites. Available at: http://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html (Accessed: 5 March 2016).

BBC News(2016) CPS to prosecute 'trolls' who use fake online profiles. Available at: http://www.bbc.co.uk/news/technology-35712772 (Accessed: 8 March 2016).

Brecht, D. (2016) Security awareness and spear phishing: How to stay out of danger. Available at: http://www.appstechnews.com/news/2015/aug/24/security-awareness-and-spear-phishing-how-stay-out-danger/ (Accessed: 11 March 2016).

Vanno (2011) Improving Questionnaire Design of Establishment Surveys for Field Data Collection. Available at: https://www.amstat.org/sections/srms/proceedings/y2011/Files/400161.pdf (Accessed: 7 March 2016).

Google (2016) Create forms. Available at: https://www.google.co.uk/forms/about/ (Accessed: 29 March 2016).

Maddem, M. (2013) Teens, Social Media, and Privacy. Available at: http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf (Accessed: 12 March 2016).

Smart Survey (2013) Advantages of using Likert scale questions. Available at: https://www.smartsurvey.co.uk/blog/advantages-of-using-likert-scale-questions/ (Accessed: 16 March 2016).

Baum (2009) Stalking Victimization in the United States. Available at: https://victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0 (Accessed: 15 March 2016).

ICO (2015) Key definitions of the data protection act. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (Accessed: 14 March 2016).

Data Protection Act1998. Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/2 (Accessed: 17 March 2016).

ICO (2015) Online safety. Available at: https://ico.org.uk/for-the-public/online/social-networking/ (Accessed: 19 March 2016).

ICO (2015) Keeping personal data accurate and up to date. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (Accessed: 19 March 2016).

Rouse, M. (2009) What is identity theft? Available at: http://searchsecurity.techtarget.com/definition/identity-theft (Accessed: 18 April 2016).

e Marketer (2013) Online banking in the UK. Available at: http://www.emarketer.com/Article/Online-Banking-UK-Trumps-In-Person-with-More-Users-More-Often/1009678 (Accessed: 24 March 2016).

Santander (2016) Santander UK. Available at: http://www.santander.co.uk/uk/index (Accessed: 28 March 2016).

Barclays (2016) Barclays UK. Available at: http://www.barclays.co.uk/ (Accessed: 28 March 2016).

TSB (2016) Loyds TSB. Available at: https://www.lloydsbank.com/ (Accessed: 28 March 2016).

Halifax™ (2016) Halifax UK. Available at: http://www.halifax.co.uk/ (Accessed: 28 March 2016).

NatWest (2016) NatWest Online UK. Available at: http://personal.natwest.com/ (Accessed: 28 March 2016).

Vahl, S. and BBC (2016) Online break-in forces bank to tighten security. Available at: http://www.bbc.co.uk/news/business-35716872 (Accessed: 25 March 2016).

Techopedia (2016) What is whaling? Available at: https://www.techopedia.com/definition/28643/whaling (Accessed: 10 April 2016).

Visual Paradigm (2016) Software Design Tools. Available at: https://www.visual-paradigm.com/ (Accessed: 2 April 2016).