



**Sudan University of Science and Technology**  
**College of Graduate Studies**  
**Faculty of Computer**



# **Proposing a User-Centered Model for Evaluating the Security of Social Media (Case Study - Facebook)**

اقترح نموذج لمستخدم لتقويم أمن وسائل التواصل  
الاجتماعي  
(دراسة حالة الفيسبوك)

A Thesis Submitted in Partial Fulfillment of the Requirement  
for the Degree of M.Sc. in Information Technology

By

**Nuria Yagoub Ahmed Elhag**

Supervisor

**Maha Abo Yousif Abo**

**Jan 2022**

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

## الآيات

قال بجلل الله: اقرأ باسم ربك الذي خلق ﴿1﴾ خلق الإنسان

من علق ﴿2﴾ اقرأ وربك الأكرم ﴿3﴾ الذي علم بالقلم

﴿4﴾ علم الإنسان ما لم يعلم ﴿5﴾

سورة العلق الآيات (1-5)

# Dedication

This thesis is dedicated to:  
The sake of Allah, my Creator and my Master,  
My great teacher and messenger, Mohammed (May Allah bless and grant  
him),  
Who taught us the purpose of life,  
The Sudan University of Science and Technology; my second magnificent  
home;  
My great parents, who never stop giving of themselves in countless  
Ways,  
My dearest family, who leads me through the valley of darkness  
With light of hope and support,  
My beloved brothers and sisters,  
My friends who encourage and support me,  
All the people in my life who touch my heart,  
I dedicate this research

# Acknowledgement

First of all, I thank **ALLAH** Almighty for blessing me with strength and patience to complete this, there is no way work to be accomplished without his generous.

O **ALLAH**, to You is praise as befit the Glory of Your Face and the Greatness of Your Might.

I honestly cannot find suitable words to express the depth of my gratitude and appreciation for **Dr.** Maha Abo Yousif Abo my supervisor whose valuable guidance and encouragement always inspired me and made my work easy enlightening my ideas.

I take the chance to greeting my solider who spend every precious and spare no effort even before my first steps to my beloved father.

## **Abstract**

The study dealt with proposing a User-Centered Model for Evaluating the Security of Social Media. The problem of the study is the existing privacy and security systems evaluation models are designed for specific system and do not take all systems in consideration. Also, the designers have created their systems depend on the general principles and guidelines so the applicability depends on the understanding of the designer. In addition, they were not involving the user during the designing security features which make problems in usability. The study aims to propose a user-centered model for evaluating security issues in social media. The study follows the descriptive approach and uses the SPSS to analyze the data. The study reach on the following results: There is a positive statistically significant relationship between security settings and their clarity, the user cannot distinguish active or turned-on security features on their account with 70%, Icons can be distinguished from each other easily with 64%. The study recommend that users have to learn how to marking which security features are active or turned on in account, users have to learn how to find out what security settings are available. Users have to make strong password.

## مستخلص

تناولت الدراسة اقتراح نموذج لمستخدم لتقييم أمن وسائل التواصل الاجتماعي. مشكلة الدراسة هي أن نماذج تقييم أنظمة الأمن والخصوصية الحالية مصممة لنظام معين ولا تأخذ جميع الأنظمة في الاعتبار. أيضًا ، أنشأ المصممون أنظمتهم التي تعتمد على المبادئ العامة والإرشادات ، لذا فإن قابلية التطبيق تعتمد على فهم المصمم. بالإضافة إلى ذلك ، لم يتم إشراك المستخدم أثناء تصميم ميزات الأمان التي تسبب مشاكل في سهولة الاستخدام. تهدف الدراسة إلى اقتراح نموذج محوره المستخدم لتقييم القضايا الأمنية في وسائل التواصل الاجتماعي. تتبع الدراسة المنهج الوصفي ، وتستخدم SPSS لتحليل البيانات. توصلت الدراسة إلى النتائج التالية: توجد علاقة إيجابية ذات دلالة إحصائية بين إعدادات الأمان ووضوحها ، لا يمكن للمستخدم التمييز بين ميزات الأمان النشطة أو المشغلة في حسابه بنسبة 70% ، ويمكن تمييز الرموز عن بعضها بسهولة باستخدام 64%. توصي الدراسة بأن يتعلم المستخدمون كيفية تحديد ميزات الأمان النشطة أو المشغلة في للمستخدم ، ويتعين على المستخدمين معرفة كيفية إعدادات الأمان المتاحة لهم. يجب على المستخدمين إنشاء كلمة مرور قوية.

# List of Contents

|                  |      |
|------------------|------|
| DEDICATION       | I    |
| ACKNOWLEDGEMENT  | II   |
| ABSTRACT         | III  |
| مستخلص           | IV   |
| LIST OF CONTENTS | V    |
| LIST OF TABLES   | VIII |
| LIST OF FIGURES  | IX   |

## CHAPTER I

### INTRODUCTION

|                                    |   |
|------------------------------------|---|
| 1.1. Introduction:                 | 1 |
| 1.2. Problem statement:            | 4 |
| 1.3. Research aim:                 | 4 |
| 1.4. Objectives of Research:       | 4 |
| 1.5. Significant of the research:  | 4 |
| 1.6. Contribution of the research: | 5 |
| 1.7 Methodology of study:          | 5 |
| 1.8 Thesis Hypothesis              | 5 |
| 1.7. Research outline:             | 6 |

## CHAPTER II

### LITERATURE REVIEW

|                       |   |
|-----------------------|---|
| 2.1. Introduction:    | 5 |
| 2.2 Related Concepts: | 5 |
| 2.3 Literature Review | 9 |

**CHAPTER III  
METHODOLOGY**

|                                 |    |
|---------------------------------|----|
| 3.1. Introduction               | 21 |
| 3.2. Research Method            | 21 |
| 3.3. population and sampling    | 21 |
| 3.4. Data collection Techniques | 21 |
| 3.4. Validity and Reliability   | 22 |

**CHAPTER IV  
DATA ANALYSIS, RESULTS AND DISCUSSIONS**

|                                 |    |
|---------------------------------|----|
| 4.1. Analysis of personal data: | 24 |
|---------------------------------|----|

**CHAPTER V  
RESULTS, RECOMMENDATIONS**

|                    |    |
|--------------------|----|
| 5.1 Results:       | 39 |
| 5.2 Recommendation | 39 |
| 5.3 References:    | 40 |

**APPENDIXES**

|              |    |
|--------------|----|
| Appendix (1) | 42 |
| Appendix (2) | 47 |
| Appendix (3) | 64 |



## List of Tables

|   |    |
|---|----|
| Table (3.1) Results of stability and Validity test for the study variables.                             | 21 |
| Table (3.2) Results of stability and Validity test for the study variables                              | 33 |
| Table (4.1) Frequent distribution of the study sample according to the age variable                     | 35 |
| Table (4.2) Frequent distribution of the study sample according to the gender variable                  | 36 |
| Table (4.3) Frequent distribution of the study sample according to the specialization variable          | 37 |
| Table (4.4) Frequent distribution of the study sample according to the account in social media variable | 38 |
| Table (4.5) Frequency distribution of the first hypothesis statements                                   | 39 |
| Table (4.6) Descriptive statistics for the first hypothesis statements                                  | 39 |
| Table (4.7) Frequency distribution of the second hypothesis statements                                  | 41 |
| Table (4.8) Descriptive statistics for the second hypothesis statements                                 | 42 |
| Table (4.9) Frequency distribution of the third hypothesis statements                                   | 44 |
| Table (4.10) Descriptive statistics for the third hypothesis statements                                 | 45 |
| Table (4.11) Chi square test for the first hypotheses   | 47 |
| Table (4.12) Chi square test for the second hypotheses  | 48 |
| Table (4.13) Chi square test for the third hypotheses   | 49 |

## List of Figures

|  |    |
|--|----|
| Figure (3.1) Figure (3.1) the proposed model to evaluate the usability of the security in social media | 26 |
| Figure (4.1) Frequent distribution of the study sample according to the age variable                   | 35 |
| Figure (4.2) Frequent distribution of the study sample according to the gender variable                | 36 |
| Figure (4.3) Frequent distribution of the study sample according to the specialization variable        | 37 |
| Figure (4.5) Responses about security settings and their visuality                                     | 38 |
| Figure (4.6) Responses about security and their learnability   | 41 |
| Figure (4.7) Responses about security setting and their applicability                                  | 44 |
| Figure (4.8) the screen of original navigation bar for Facebook:                                       | 47 |
| Figure (4.9) the screen of proposed navigation bar for Facebook:                                       | 50 |
| Figure (4.10) the screen of proposed navigation bar for Facebook:                                      | 51 |

## List of Abbreviations

| <b>Abbreviations</b> | <b>Full Form</b>                         |
|----------------------|--|
| <b>IT</b>            | Information Technology                   |
| <b>HCI</b>           | Human Computer Interaction               |
| <b>USEC</b>          | Usable Security                          |
| <b>GOMS</b>          | Goals, operators, methods, and selection |
| <b>HCISec</b>        | Human Computer Interaction Security      |

**CHAPTER ONE**  
**INTRODUCTION**



## **1.1. Introduction:**

It is widely acknowledged that one of the most important research areas for computer security today is the development of techniques that will make security systems easier to use—and correspondingly make easy-to-use systems more secure. (Yeratziotis, Van Greunen, and Pottas, 2012). "A chain is only as strong as its weakest link." To realize security within the realm of human computer interaction, the weakest link, namely the human should be strengthened (Napoli, 2018). Also many users enter sensitive information of unprotected websites because they lack the knowledge or skill to distinguish between a secure and insecure website. Users knowledge or skill level a major role in the secure of a system (Napoli, 2018).

Secure human computer interaction is a much-desired feature for E-commerce environments and all IT products. Users want to have the assurance that the interface through which they enter their credit card information, for an electronic transaction, will provide the necessary information security services to protect their information against unauthorized reading and modification. Successful and secure human computer interaction is further dependent on features such as the user seeing and understanding how his credit card information is secured when using the interface. The three main components in human computer Interaction are humans, computers and how they relate to each other.

In HCI realm a popular quotes state that any feature of a software considered not present if not designed properly to take up by user. A security and privacy solution must be easily updateable to contain changes in legislation and regulations on a regular basis in various sectors (such as health care, banking, government), there are distinct requirements ,and the software is designed to be easily controlled when updating efficiently (Chiasson and Biddle, ,2007). HCISec specializes in designing and evaluating interactive security systems (Thirty, 2005). When designing, the dominance should be in favor of the user's mental model, and it should support the creation of accurate models to represent the cybersecurity interface. Cybersecurity should provide a smooth and satisfying operation through the interface. Although some modifications were made to the interface to enable the user to customize it to a certain extent (Ferreira and J. Anacleto, 2017), it was noticed that there were an increase in crashes and cyber-attacks on these systems.

Many security breaches are not due to failure of technologies, but rather to failure in user-friendly security design on the user interface, hence the role of HCISec, which relies on a range of related disciplinarians to support user-based systems to enhance the security aspect in terms of practice. The National Academy of Engineering and the CRA (Computer Research Association) declared usable security to be a major challenge, so similar methods of Cognitive Heuristics and Guidance and GOMS had

to be devised (clare-marie, carolyn, and john, 2006). The effectiveness of the application of cybersecurity and its usable tools play a key role for guidance, for example, in addressing errors, assistance, and suggested steps to solve problems (Ferreira and J. Anacleto, 2017).

As social media platforms have grown in number and size over time, this means that there is more information on the web and therefore not translated only more invasion of privacy but more theft, corruption, misuse and manipulation with personal information and that is what is realistic phishing is still the first threat action and is used in social media related attacks. Hence user should carefully aware about is his information security and the consequences of fraudulent cyber activity without frustration. Most social platforms were not focus primly on designing features to enhance cybersecurity through interface neither in term of their clarity nor their applicability. The lack of studies in field HCISec play a key role in these issues.

Noteworthy: Fundamentally, users will work around anything necessary to get their job done which means usable security has to get user where they want not just block unsafe actions in addition to be motivated to take care of security (Molich and Ballerup,1990). Use of Icons as a Visual Indicator: Most users are quite commonly affected by use of any kind of pictures as well as icons in any of the interfaces (Napoli, 2018).

## **1.2. Problem Statement:**

1. The existing privacy and security systems evaluation models are designed for specific system and do not take all systems in consideration.
2. The designers have created their systems depend on the general principles and guidelines so the applicability depends on the understanding of the designer
3. They were not involving the user during the designing security features which make problems in usability.

## **1.3. Aim of Study:**

The aim of this study is to propose a user-centered model for evaluating security issues in social media

## **1.4. Objectives of the Study:**

- To analyze the existing HCI-SEC systems to find the user-centered criteria.
- To propose the User-Centered HCI-SEC model based on the above criteria.
- To compare the proposed model with the other existing security models.
- To identify barriers related to usability of social media security
- To suggest an enhanced social media UI comply with the proposed model

## **1.5. Significance of the Study:**

Help secure systems, websites, and applications that provide understandable feedback to users by evaluating security features and current system status. In addition ensure that the users will

response with suitable way, and clear model for designers to follow to maintain product security.

### **1.6. Contribution of the Study:**

Contribution of this thesis in the usable security realm toward better understanding and design

### **1.7. Methodology of Study:**

The model is constructed from previous works, which is taking into account the USEC criteria or at least both usability and security most frequently used (visibility for state of security and functionality, convey features with figures and pictures, aesthetic and minimalistic design (Johnston, Eloff, Labuschagne, 2006) clarity(John, Jodi, Shelley, 2007), inclusivity of users (Helen, 2006), learnability (Andrea, Tiziana, 2018), path of least resistance (Rodney, Ross, 2004), inclusivity (Julio, Luis, 2007), navigability (Nigel ,2001),and user control (Blaine, Karim, Bashar, 2005)). The model is constructed from the following steps:

1. Collecting (trade off) the needed security features.
2. Classifying these features into three classes each class present the security and how the user get benefits from it.

### **1.8. Thesis Hypothesis:**

- There is a statistically significant relationship between the use of security settings and their clarity



- There is a statistically significant relationship between the use of security settings and the ease of teaching them
- There is a statistically significant relationship between the use of security settings and the ease of their application

### **1.8. Thesis Outline:**

The outline of this research is as follow:

Chapter one contains an introduction about HCI and security, problem statement, methodology and tools, study objectives, thesis aim, significant of the study, contribution of the study and thesis outline. Chapter two highlight literature review about usable security issues with guidelines, models and evaluation, chapter three illustrates the methodology followed in this thesis , chapter four describe results, and chapter five points the conclusion and recommendations.

**CHAPTER TWO**  
**LITERATURE REVIEW**

## **2.1. Introduction:**

This chapter is about discussing of state-of-the-art in this thesis area to define the properties that are used as guideline in the previous works. Hence, this chapter has been divided to two parts: the first part is about the related concepts, which are necessary to understand this thesis work. The second part is containing literature review and providing a summarization for most of related works.

## **2.2. Social Media:**

Social networking sites mean any platform used to facilitate the transfer, sharing and interaction of content between its users through an application or browser using a computer or mobile devices (techtarget.com, 2021) or social media refers to all computing that is concerned with the user, his interactions, and his content (Kaplan and M. Haenlein, 2010 ). (Terry, 2009) The social platform is described according to its orientation, the tools it provides, and the forms of interaction such as Facebook and Twitter or messages (Howard and Parks, 2012). (Russo et al, 2006) defined it as any intermediary technology used to spread content and ideas through networks or digitize traditional forms of communication (Lewis et al, 2010) .The problem in the previous definitions lies in that it does not include the modern interaction patterns contained in social media, so both Howard and Parks (Howard and Parks, 2012 ) provided a more comprehensive definition than three sections : (a) the

information infrastructure and tools used to produce and distribute content; (b) the content that takes the digital form of personal messages, news, ideas, and cultural products; and (c) the people, organizations, and industries that produce and consume digital content.

### **2.3. Usable Security:**

Usable Security (USEC) concerns with looking for appropriate ways to access the resources safely using a usable user interface. Usable Security (Usec) is the field that investigates these issues, focusing on the design of security and privacy features that are easy to use. It focuses on making security more usable (user-friendly) on websites without compromising the security itself (Yeratziotis, Van Greunen, and Pottas, 2012). The field of usable security emphasizes the value of assessing and integrating user behaviors within the design of security mechanisms (Napoli, 2018). In addition, it is the field that looks at the difficulties that users face when interacting with security. USEC is the area that looks at these issues, pay attention to designing security and privacy features that are usable. The emerging area of privacy and usable security is based on ideas from HCI, computer security, and many other sciences, to come up with human-centric systems to manage security and privacy that are powerful in practice (Yeratziotis, Van Greunen, and Pottas, 2012). The field of usable security has primarily focused on designing user interfaces for end-users. These users have little knowledge about

computer security and their focus is not on completing security tasks, the field of usable security recognizes that to be secure, a system must be usable (Chiasson and R. Biddle, 2007). The usable security field is based on HCI and other sciences and aims to develop human-centered systems to optimize the use of privacy and security in practice (Yeratziotis, Van Greunen, and Pottas, 2012). Whitten and Tygar (Thirty, 2005) defined the usable security through software product that meet users enough knowledge to deal with required security ability to perform the successful task accomplishment recognizing the errors that compromise the security during performing the task with acceptable effort and easiness. Usable security or human-computer interaction and security (HCI-Sec) is a field of research that aims to unite usability and security concepts in order to provide secure solutions that can be usable by users (Ferreira and J. Anacleto, 2017). The domain considering human aspects related to security and the integration of usability with security is known as usable security (Synthesis Lectures on Information Security, Privacy and Trust, 2020).

#### **2.4. Evaluation:**

Many Systematic, rigorous, and meticulous application of scientific methods has been developed to assess the design, implementation, improvement, or outcomes. These methods were used to evaluate interfaces and systems to determine how usable they are for different user groups – identify good and bad

features to inform future design – compare design choices to assist us in making decisions – observe the effects of specific interfaces on users. Most of these approaches are user studies and expert-based evaluation techniques. In the user studies methods, a representative sample of users is recruited to participate in experiments to test a system’s usability. Specific examples of user studies include laboratory-based user testing, questionnaires, interviews, and observing users and recording and assessing system use. Within the expert-based evaluation technique, usability experts assess and inspect usability aspects of a system using their knowledge and a range of usability rules and heuristics (rules of thumb).

#### **2.4.1 Heuristic Evaluation:**

Heuristic Evaluation (HE) is the method for finding usability problem and systematic inspection to see if interface complies with guidelines works for paper, prototypes, and working systems (Molich and Ballerup, 1990). A heuristic evaluation is regarded as an analytical evaluation method, which is undertaken by usability experts. The experts apply a specific set of heuristics to evaluate the usability of a user interface. The method is widely used because it is an excellent method of diagnostic and perspective analysis for identifying individual problems in a short time period. Specifically, its purpose is to identify problems that are associated with the design of user interfaces. The results are dependent on the experts’ broader experience

with usability. The HE is an effective method to review interfaces by taking the recommendations based on User Centered Design (UCD) and contrasting them with the applications. These recommendations come in different ways, such as design principles, heuristics, guidelines, user interface design patterns and standards that can be used by interface designers and evaluators .Heuristic evaluation is an inspection method in which the main characteristic is that there are experts (known as evaluators) that evaluate aspects of the system interface related to usability and security (Realpe-muñoz et al, 2017). Heuristic evaluation is considered as a method of inspection of analytical evaluation, It is the best-known usability inspection techniques and was developed by Jakob Nielsen of bell labs and after SunSoft Nielsen determined heuristic evaluation as a systematic inspection of the user interface by the observation of an interface and in finding good and bad things, usually performed by evaluators who can use certain documented rules (guidelines). HE is a usability engineering method “for finding usability problems in a user interface design by having a small set of evaluators examine the interface and judge its compliance with recognized usability principles (Nielsen et al, 1994).

### **2.5. HCI-Security:**

HCISec’s primary focus is on legitimate users’ mistakes that may compromise the system. HCISec is concerned with threat

scenarios, undesired actions that may cause non-malicious users to break the security of system (Kainda, I. Flechais, and A. W. Roscoe, 2010), security HCI (HCI-S) has recently being introduced to reflect the need to explicitly support security in the UI development life cycle (Johnston and Eloff, 2003) .The concept of HCI-S modifies and adapts the concepts of the traditional HCI to focus in aspects of security and to find how to improve security through the elements of the interface. HCI-S definition proposed by (Johnston et al, 2003) ,which textually reads “The part of a user interface which is responsible for establishing the common ground between a user and the security features of a system”. HCI-S is human computer interaction applied in the area of computer security, HCI-S deals with how the security features of the UI can be as friendly and intuitive as possible, because of the easier a system is to use, the less likely is that the user will make a mistake or try to bypass the security feature, resulting in a more reliable system. Human-Computer Interaction and Security HCISec arise because of the need that was identified by Human-Computer Interaction (HCI) experts to improve the usability of secure systems. Flechais (Flechais, 2005) pointed out that HCISec is focusing nearly exclusively on improving the user interface of secure systems; while he recognizes the importance of the user interface in making a secure system usable.



## **2.6 Literature Review**

(Yeratziotis, Van Greunen, and Pottas, 2012) In this study, a framework was studied in the context of social networks within the health domain. The framework consists of three components: a three phase process, a validation tool and a usable security heuristic evaluation. They believe that theories and evaluation tools for usable security, including guidelines and principles, are limited and those that exist are at an elementary and progressive stage. As a result, developers struggle to design security and privacy that is usable.

(Yeratziotis et al 2012) suggested framework containing three components to evaluate usable security in online social networks of usable security heuristic evaluation, a three-phase process to develop heuristics for specific application domains and a validation tool. It must be noted that each phase of the process has a number of tasks. The usable security heuristic evaluation represents the selected usability inspection method and the process to develop heuristics for specific application domains as an approach that will be used to develop the method itself. The validation tool is used to determine the validity and applicability of the method. In addition, a case study on two online health social networks was conducted to determine the validity and applicability of both the approach and the method. This will be achieved by ensuring that security and usability form a unified process that is considered in user interface design.

The author (Kayhan Sayin, 2019) proposed a security and usability threat model detailing the different factors that are pertinent to the security and usability of secure systems, together with a process for assessing these systems. A complete evaluation must consider factors that may affect security as well. A security threat model that encompasses elements of usability as a difficult-to use system may force users to resort to insecure behavior such as circumventing security processes—making protected assets insecure. The security-usability threat model depicts the critical factors that need investigation during the evaluation of usability and security. It identifies factors that are related to either usability or security and also factors that are related to both. Both security and usability factors relate to the legitimate user who has no malicious intent to harm the system. In addition, they use the concept of usage scenarios (or simply scenarios) and threat (negative) scenarios. Usage scenarios have been defined as actions that are desirable to stakeholders of a secure system and threat scenarios as actions that are not desirable and hence the system should not allow them to happen.

The authors in (Yeratziotis et al, 2012) developed a usable security heuristic evaluation for measuring the usability of security and privacy features on online health social networks. The objective of the developers is to define a process to design HEs for Specific Application Domains (SAD). They consider both of these themes. Firstly, it attempted to develop a USec HE,

which is corresponding to the theme of developing new heuristic sets for specialized domains. Secondly, it provided a new process for creating a HE for a specialized domain, which helps to push the way of heuristic evaluation to advanced level.

Yasser (Yasser and Allen, 2014) proposed an Assessment Framework for Usable-Security (AFUS) in the decision science branch he used the benefits of two famous techniques. AFUS explored the benefits of using two well-known techniques from Decision Science, namely Utility Functions and Decision Trees, for assessing the balance between security, usability and usable security represented in the set of requirements for a particular software product. To generate a metric that developers can use to gauge the balance between the attributes. They assume that the developers of a product are aware of the balance between security and usability that is appropriate for their product, thus the proposed technique is intended to assist in reaching that desired balance. As changes to the requirements are made, reassessment using AFUS can indicate if the product has shifted to a greater emphasis on one attribute at the expense of the others, or if all attributes have moved towards the developer's preferred equilibrium.

In (Mihajlov et al, 2011) a framework have been introduced take into account how far the user could authenticate to the system under specified context to evaluate usable security through reconciliation of quality metrics the framework specify the

quality metrics according to two principles: participation and categorization. They Building on previous works, which is focusing on usability perspectives in more detail. The authors presented a mathematical approach that derives a total quality score for usable security in a security system conceptual framework includes the 5 security characteristics and 5 usability characteristics, then quality criteria computed individually to determine total quality of the system.

The framework in (Furnell and Katsabas, 2007) generated from elicited of results testing users through set of activities as web serving, text editor and email services. Experiences included a novice and skilled users. The participants were showed tasks by written and explained manner, the typical tasks selected to the users uncover complicated to be understood neither when they are dealing with basics security that are required by the concerned applications nor by the users whose have desire to customize setting. They were informed about the goals should be reached during activities without specify how to achieve, to understand their behavior about using the available features to get job done. They were permitted to utilize the online help alongside with that one to accompany on the application.

In (Nurse et al, 2011), the authors focused on the software from view point of user on how to use security which are available in applications they usually use it. Authors believe that paying attention of usability of security features in early stages of

development of any software product will guide to well learning of the benefits of security services, noteworthy these services must be accessible to user. The examples argued are evaluated against criteria the authors identified.

In (Eloff, 2002) the author equip with many of already used guidelines to design, and a basic set for use it later as reference. With cases and troubles which appear and evaluations methods all relevant about cyber security usability to take closer look of the HCISec field specially when is about recommendation for usable security.

The authors in (Realpe, Collazos, and Granollers, 2016) argued about how much the security are usable equipping a list of 153 heuristics on scale of how much the desired characteristic achieve the performance, accessibility, operability and reliability on user authentication, the authors whose making of these heuristics in interrogative form aimed to help in improving and practicing the evaluation to get standardization .for more facilitation they provide each of heuristics with comments for explanation. The list provided is has reviewed by a number of experts in HCI, information security and usable security.

In (Katsabas, Furnell and Phippen, 2005) many present applications were rated to determine the level of their compliance against identified principles created, these principles were elicited from standards that of HCI in order to guide the

insertion of the security features inside applications .the guidelines created were used to evaluate applications.

In (Realpe-munoz et al, 2017), they presented a preliminary process for designing secure and usable systems using a user-centered approach. The process called MPIu+ approach is used to gain not just usable but also include the security aspects for interactive systems. The model taking into account the most important aspects of requirements analysis, design and evaluation with respect to usable security and that it can contribute with its trade-off requirements analysis, design and evaluation.

In (Fidas and Avouris, 2010), they proposed a user-centric approach towards achieving “usable security”. As a case study they apply the proposed approach on the password management problem.

In (Yee, 2002),the author established some starting points for reasoning about security from a user-centered perspective: To view the system according to the concepts of the actors and his ability .He came up with new principles and real examples to proof it functionalities in secure interaction .

In (Hof, 2015), guidelines introduced to help developers handling issues that arise to the user when he deals with security features. To underline the importance of the presented guidelines, weaknesses of security mechanisms in common applications regarding usability for end users are shown in an

analysis of common applications and security mechanisms on basis of the presented guidelines.

(Jayalakshmi Raman et al, 2018) They formed a framework generic that based on the specifying main ideas related to CAPTCHAs the. Authors reviewed cases that emerged when using CAPTCHAs to inspect the usability problems authors propose use their framework to both evaluation and design for well guide about CAPTCHs. They consider the identified main concepts (content generality, presentation, and complexity) of the generic framework and break them down to sub attributes to fit all users, authors try to include schemes, frameworks, usability issues, evaluation and distinguishable usability features to obtain a good look at CAPTCHAs to achieve the framework depending on a quantitative method which is a phased method.

Daniela (Napoli, 2018) has conducted inspection by many ways in journal articles and conference papers to extract the most common points from. Then use the recommendations, best practices and behaviors then categorize for developing their heuristics in try to reveal troubles obstacle the user understanding and commit it. The author proposes heuristics to serve the design and evaluation for usable security and get the result of the work are recommended for usable security in case of non-visual use. Ten websites were evaluated against identified heuristics through assigning standard tasks to achieve the results

uncover many of problems specifically for users with vision-loss.

In (Alarifi et al, 2017) they argued about current frameworks and it's applicability to meet basic requirements for usable security, after conducting literature review they came up to a new model with new metrics were not mentioned on previous works beside the existing metrics, the authors pointed that even ISO and NIST have missed some essential metrics in terms of evaluating the portals of E-banking and is not comprehensive. To prove their view the evaluation was conducted by the new model on five big banks. The case study evaluation reveal issues about learn about common attacks, best practices for online security, authenticating and alerts while no banks inform their customers about the known key logger which are has serious consequences.

## 2.4 Summary of Related Work

Table 2.1 Summary of related work

| Author  | Method   | Criteria  | Case study   |
|---|--|---|--|
| A. Yeratziotis, D. van Greunen and D. Pottas    | usable security heuristic evaluation<br>A three-phase process to develop heuristics<br>A validation tool | Visibility, revocability, clarity, learnability, aesthetics ,Minimalist design ,Errors ,user suitability, user Language, user Assistance, Identity Signal ,Security and Privacy                                       | evaluate usable security online social networks to the health domain |
| Ronald Kainda and Ivan Flechais and A.W. Roscoe | use the concept of usage scenarios (or simply scenarios) and threat (negative) scenarios                 | <b>Factors of usability:</b><br>Effectiveness, satisfaction<br>Accuracy, efficiency, memorability, knowledge/skill<br><b>Factors of security:</b><br>Attention, vigilance, Conditioning, motivation<br>social context | _____  |



|   |   |  |       |
|---|---|--|-------|
| Darelle Van Greunen, Alexandros Yeratziotis, Dalenca Pottas       | Phase 1: Design high-level heuristics<br>Phase 2: Validation of high-level heuristics<br>Phase 3: Application/usage of high-level heuristics  | Nielsen developed the “ten usability heuristics” (Nielsen, 2006) and Xerox the “HE - system checklist” (Pierotti, 1995).   | _____ |
| Yasser M. Hausawi and William H. Allen                            | <b>Quantitative method:</b><br>Requirements filtering and merging, utility functions and Decision trees   | <b>Security properties:</b><br>Confidentiality, Integrity availability<br><b>Usability properties:</b><br>Effectiveness, efficiency user satisfaction  | _____ |
| Martin Mihajlov, Saso Josimovski, Borka Jerman-Blazič             | Mathematical evaluation by determining SQ and UQ is based on the values of security and usability criteria respectively each is dependent on 5 variables. To calculate the quality dimension take the square-root of the sum of all squared criteria for the particular dimension | <b>Security evaluation:</b><br>Secrecy, abundance, revelation, privacy and breakability<br><b>Usability evaluation:</b><br>Meaningful retrieval, Processing depth, Requirements, Convenience, Inclusivity. | _____ |
| M.M. ELOFF, J.H.P. ELOFF  | Compare interfaces relating to information security against five defined criteria   | Complexity, visibility, Interaction, unambiguous, Information security awareness facilitated, and which information security services are addressed by the interface                                       | _____ |
| Jason R. C. Nurse, Sadie Creese, Michael Goldsmith, Koen Lamberts | review of pertinent cyber security usability issues and evaluation techniques applied, refined list of general 19 guidelines drawn from the literature  | Accommodate many criteria  | _____ |

|   |  |  |  |
|---|--|--|--|
| Paulo C. Realpe, Cesar A. Collazos, Julio Hurtado, Antoni Granollers                              | A set of 153 heuristics experts is presented. The heuristics are gathered in 6 attributes o characteristics.   | <b>Usability</b> :visibility, simple design, user control, match the real world, recognition rather than recall, help users recover from errors, efficiency of use, error prevention, consistency, documentation, convey features<br><b>Security:</b> Integrity, authenticity, confidentiality, non-repudiation, privacy |  |
| Paulo Realpe-Muñoz, César A. Collazos, Toni Granollers, Jaime Muñoz-Arteaga, Eduardo B. Fernandez | Requirements analysis, design and Evaluation   | Nielsen’s heuristics, accessibility, operability, reliability, Performance   | _____  |
| M. Nohlberg and J. Bäckström  | Interviews and scenario testing to construct "low-fi" prototype on paper and " high-fi" prototype then get the design and heuristics                               | Provide overview information very early in the program, do not overwhelm the user, provide information in a way that is familiar   | An interview was made with representatives from the sponsoring company, Siguru |
| Ka-Ping Yee   | Actor-ability model and a set of design principles.  | Path of least resistance, active authorization, revocability, visibility, self-awareness, trusted path, expressiveness, relevant boundaries, identifiability, expressiveness, Clarity  |  |
| Hans-Joachim Hof  | Guidelines that help software developers to improve end user usability of security-related mechanisms, and analyzes common applications based on these guidelines. | <b>Understandability</b><br>open for all users<br><b>Empowered users:</b><br>No jumping through hoops, efficient use of user attention and memorization capability, only informed decisions, security as default, fearless System, security guidance, educating reaction on user errors, consistency                     | _____  |
| D.Katsabas, S.M.Furnell and A.D.Phippen   | Applications were tested according to the level of compliance with each of the 10 guidelines. The grading method was   | Visible system state and security functions, security should be easily used, suitable for advanced as well as first time users, avoid heavy use of technical vocabulary or advanced terms, handle errors appropriately, allow customization without risk to be   | Three antivirus applications were used also two firewall applications,         |

|   |  |  |  |
|---|--|--|--|
|   | used for all the applications and the grades were from 0 to 5 from identified table.   | trapped, easy to setup security settings, suitable help and documentation for the available security   | as well as two web-browsers.   |
| Daniela Napoli  | Using the ACCUS heuristics, one researcher with expertise in web accessibility and usable security assessed 10 websites that allowed users to exchange sensitive information | Informative, reliable, recognizable, assistive, functional, controllable, responsive, diverse and memorable  | _____  |
| Oleksandr Gordieiev, Vyacheslav Kharchenko, Kate Vereshchak | Quantitative analysis of U&S interaction. analysis for separate sub characteristics of U&S characteristics.  | <b>Usability sub-characteristics:</b> Appropriateness, recognizability, Learnability , Operability , User error protection , User interface aesthetics ,and Accessibility<br><b>Security sub-characteristics</b> Confidentiality, Integrity, non-repudiation , accountability and Authenticity | Web-site of Banking University which is on the stage of the development. They calculate metrics of significances for web-site before making changes in this web-site |

From the literature review was observed there is a need to link the security features with the concepts of actions to apply the appropriate heuristics, which means in the current interface may/may not require a security action but still need to inform about security status, so it will be more task oriented and that's insure the suitable tradeoff between usability and security without overwhelm the user. The model provides heuristics and

sub heuristics which are categorized into classes according to security actions.

## **CHAPTER III METHODOLOGY**

### 3.1. Introduction

The aim of this chapter is to describe the design and methodology used in conducting this study. It provides details about research proposed model to follow, population; participants, data collection, procedures and instruments used in this study. The questionnaire is the tool of data collection in this study. The reliability and validity of these tool is presented comprehensively. It concludes by explaining the type of data analysis and ethical concerns.

### 3.2. Proposed Model:

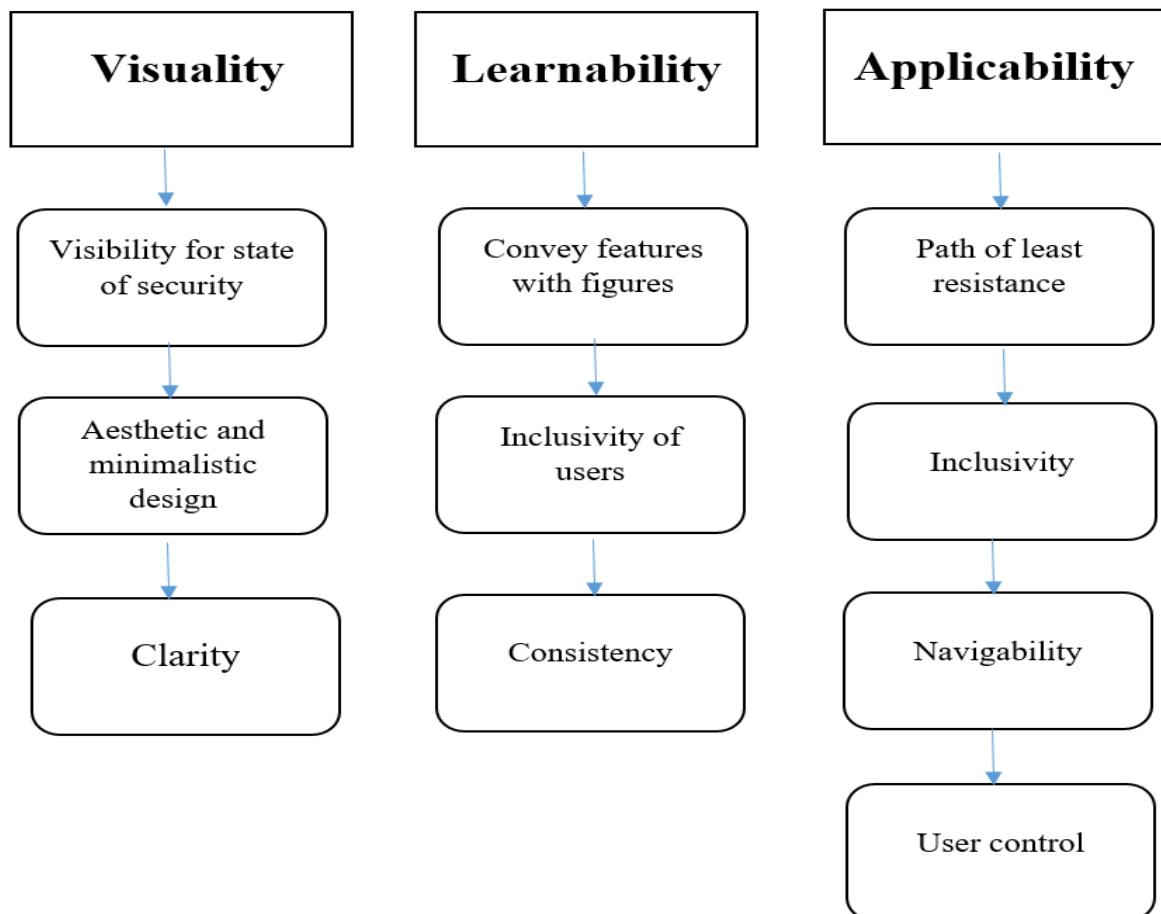


Figure (3.1) the proposed model to evaluate the usability of the security in social media

The model constructed from previous works, which is taking into account the USEC criteria or at least both usability and security most frequently used. The model is constructed from the following steps:

1. Collecting (trade off) the needed security features.
2. Classifying these features into three classes each class present the security and how the user get benefits from it. First Class Visuality contains features of security to make user more aware and protected. Second Class Learnability contains features when user wants to know more about available security. Third Class Applicability contains features when the user required a security action.

### **3.2.1. Class Visuality**

This Class contains the security features which are not requiring an action from user. It is used to convey the enabled features and the state of the current security. Class Visuality contains the following heuristics:

- 1. Visibility for state of security and functionality:** the system should keep users informed about their security status, which are as:
  - a. Notifications to identify the enabled and disabled security mechanisms.
  - b. Inform the user the type of security protocol.
  - c. Indicator for security level.

d. Display the available security features.

**2. Aesthetic and minimalistic design:** the system should apply appropriate visual representation of security elements and not provide irrelevant security information, which means:

a. Security information relevant and avoid technical words.

b. Security icons should be identifiable and distinguishable.

**3. Clarity:** the system should use plain language that users can understand with regard to security, which means:

a. Different words to convey the same idea could confuse to users.

b. Security messages should be stated in a consistent and appropriate language.

c. Security information presented should be clear and easy to understand.

### **3.2.2. Class Learnability**

Second Class contains the required features to utilize the user when asking about security related or specific action, help him to know more efficient and satisfaction in illustrated manner for easy learn. It contains the following heuristics:

**1. Convey features with figures and pictures:** the UI needs to convey the available security features to the user clearly and

appropriately; a good way to do it is by using figures or pictures, which means:

- a. Users can view the security information (textually or graphically) according to their preferences.
- b. Consistent and standards-based information is easier to be learned and remembered.
- a. Visual elements that allow the user to know privacy policies about the use of the security features are easier to be showed.

**2. Inclusivity of users:** all content and context is communicated in a way that can accommodate various abilities, which means:

- c. Presenting information appropriate for beginners and experts
- d. Helping people to operate when they have disabilities

**3. Consistency:**

- a. Consistent set of security controls and located in specific places.
- b. Security questions and answers made by the user are presented in a list.
- c. Process should be intuitive and effortless extra

### **3.2.3 Class Applicability**

The last Class contains security features that require actions from user that may include the authentication mechanisms, custom



security setting, response to security alert, and security related decision. It contains the following heuristics:

**1- Path of least resistance:** the most natural way to do any task should also be the most secure way.

- a. Method must be performed in the shortest possible time
- b. Policies to generate passwords are secure and the cognitive workload of users is minimal
- c. Provide users with alternatives to authenticate.
- d. The system can use alphanumeric characters (e.g. passwords) and graphics.

**2- Inclusivity:** ensures that everyone, regardless of hardware and software requirements, cognitive, mobility, sensory skills, can use the website.

- a. The user can use shortcuts or commands to common security task
- b. security-related error messages is suitable for novice and expert users
- c. Hardware and software requirements are minimal.

**3- Navigability (guidance):** the system should make security help relevant and apparent to users.

- a. Security-related messages should guide to resolve the problem
- b. The help information for a specific situation should follow suitable steps to fix any problem

- 4- User control:** The site is compatible with assistive technology. The interface offers robust and customizable means to protect users with various needs.
- a. Users can choose the authentication method or combinations of them.
  - b. The security level could be changed according to the abilities and preferences.

### **3.3. Study Method**

This thesis adopted the descriptive analytical method. The whole research describes phenomena and analysis the results. The study is conducted for the students of different universities, with different specializations.

### **3.4. Population and Sampling**

In this study, the population was (107), universities students with different specializations.

### **3.5. Data Collection Techniques**

The items of the questionnaire are mainly developed based on the research objectives and research questions.

#### **3.5.1. Questionnaire**

The questionnaire is a basic tool and plays an important role in gathering information. The questionnaire was well designed by the researcher with cooperation with the supervisor. The questionnaire consists of three hypotheses.

### 3.6. Validity and Reliability

**Cranach's alpha method: -**

#### **(A) Stability Test:**

Stability means the stability of the scale and its non-contradiction with the same, i.e., the scale gives the same results with a probability of equal to the value of the parameter if it is applied to the same sample. It is used to measure the stability of the "Cronbach, Alpha", according to the following equation:

$$\alpha = \frac{k}{k-1} \left[ 1 - \frac{\sum s_i^2}{s_i^2} \right]$$

Where (k) is the number of test words

(k-1) Number of test words - 1

( $\sum s_i^2$ ) The variation of the scores of each test vocabulary

) $s_i^2$  The total variance of the total test vocabulary

The value of the Cronbach coefficient is between zero and one true. If there is no constant in the data, the value of the parameter is equal to zero. Increasing the coefficient of alpha Cronbach means increasing the reliability of the data than the opposite of the sample results on the study population.

#### **(B) Validity Test:**

Validity is a measure used to determine the degree of sincerity of the respondents through their answers on a given scale. Validity is calculated in many ways, including the square root of the stability coefficient. The value of Validity and stability ranges

from zero to the correct one. Self-Validity of the questionnaire is the measurement of the tool. The validity of the tool to measure what was set for him (researcher) to find self- Validity statistically using the equation of self- Validity is:

$$\mathbf{Validity} = \sqrt{\mathbf{Stability}}$$

The following is a table showing the results of the stability and honesty test for all the study hypotheses:

Table (3.1) Results of stability and Validity test for the study variables.

| Hypotheses        | Number of items | Stability | Validity |
|-------------------|-----------------|-----------|----------|
| Frist Hypotheses  | 7               | 0.61      | 0.77     |
| Second Hypotheses | 6               | 0.78      | 0.88     |
| Third Hypotheses  | 8               | 0.70      | 0.84     |
| Total             | 21              | 0.70      | 0.83     |

Table (3.1) shows that the values of stability for all study variables are greater than (60%). These values mean the availability of a high degree of internal stability of all hypotheses of the questionnaire. It is therefore possible to say that the standards adopted by the study have internal stability. These answers are to achieve the objectives of the study and analyze the results.

And that the values of Validity for all the variables of the study is greater than (70%) and this result refers to the efficiency of the questionnaire and its ability to what is required of honest and consistent results.

**CHAPTER FOUR**  
**DATA ANALYSIS, RESULTS AND**  
**DISCUSSIONS**

## 4.1. Introduction

This chapter about data analysis and results for this study according to many variables age, gender, specialization and accounts on social media, then make hypotheses to validate mathematic relation between security and each class

## 4.2. Analysis of Personal Data:

### 4.2.1. Age:

Table (4.1) frequent distribution of the study sample according to the age variable

| Age                | Frequency  | Percentage  |
|--------------------|------------|-------------|
| Less than 20 years | 13         | 13%         |
| 21 – 30 years      | 54         | 54%         |
| 31 – 40 years      | 29         | 29%         |
| 41 – 50 years      | 4          | 4%          |
| <b>Total</b>       | <b>100</b> | <b>100%</b> |

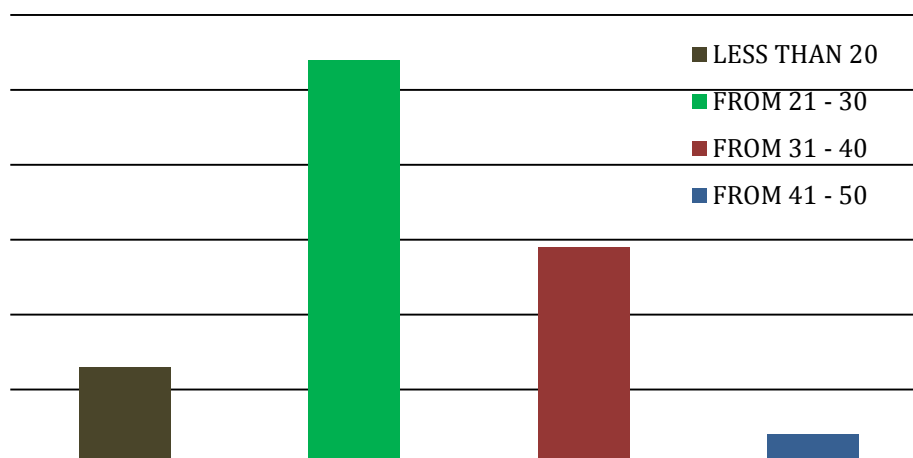


Figure (4.1) frequent distribution of the study sample according to the age variable

According to the table and figure (4.1) 13% are less than 20 years, 54% are 21 to 30 years, 29% are 31 to 40 years, and 4% are 41 to 50 years.

#### 4.2.2. Gender:

Table (4.2) frequent distribution of the study sample according to the gender variable

| <b>Gender</b> | <b>Frequency</b> | <b>Percentage</b> |
|---------------|------------------|-------------------|
| Male          | 48               | 48%               |
| Female        | 52               | 52%               |
| <b>Total</b>  | <b>100</b>       | <b>100%</b>       |

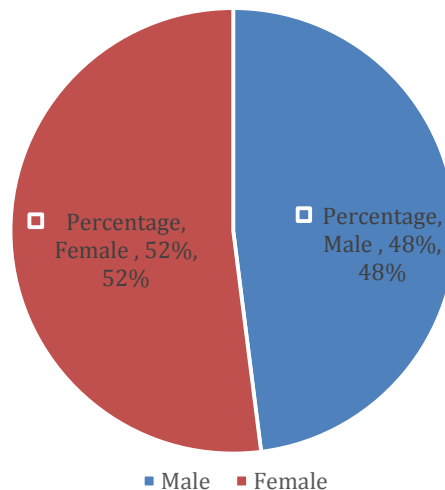


Figure (4.2) frequent distribution of the study sample according to the gender variable

According to the table and figure (4.2) 48% are male and 52% are female. The researcher noticed that the female are majority than male.

### 4.2.3. Specialization:

Table (4.3) frequent distribution of the study sample according to the specialization variable

| <b>Specialization</b>       | <b>Frequency</b> | <b>Percentage</b> |
|-----------------------------|------------------|-------------------|
| Medical and health sciences | 26               | 26%               |
| Engineering                 | 14               | 14%               |
| Economic and management     | 8                | 8%                |
| Computer science            | 18               | 18%               |
| Science and technology      | 10               | 10%               |
| Arts                        | 7                | 7%                |
| Law                         | 3                | 3%                |
| Other                       | 14               | 14%               |
| <b>Total</b>                | <b>100</b>       | <b>100%</b>       |

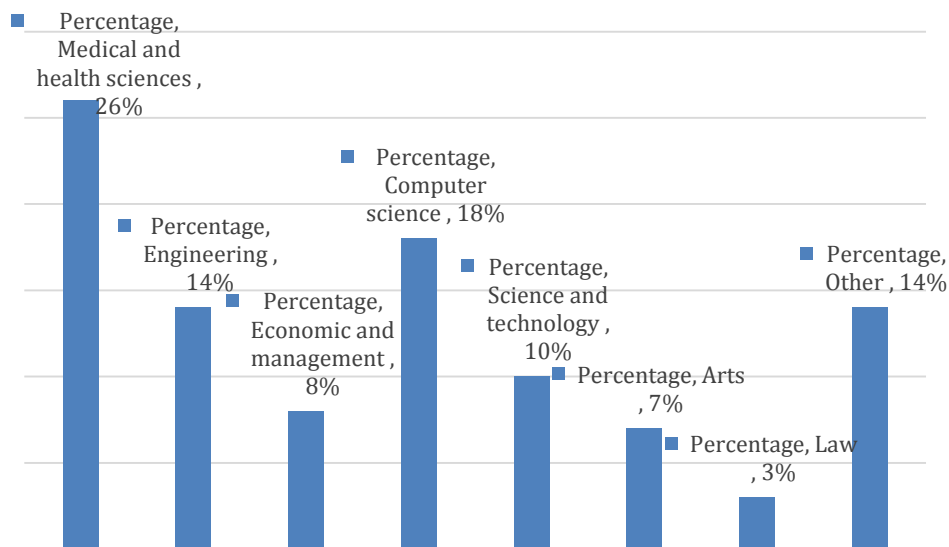


Figure (4.3) frequent distribution of the study sample according to the specialization variable



According to the table and figure (4.3) 26% their specialization is medical and health sciences, 18% their specialization is computer science, 14% are holding engineering and also other specializations are 14%, 10% are holding science and technology, 8% are holding economic and management studies, 7% are holding arts and 3% are holding law.

#### 4.2.4. Account in Social Media:

Table (4.4) frequent distribution of the study sample according to the account in social media variable

| <b>Account in social media</b> | <b>Frequency</b> | <b>Percentage</b> |
|--------------------------------|------------------|-------------------|
| Facebook                       | 93               | 93%               |
| Twitter                        | 4                | 4%                |
| Instagram                      | 3                | 3%                |
| <b>Total</b>                   | <b>100</b>       | <b>100%</b>       |

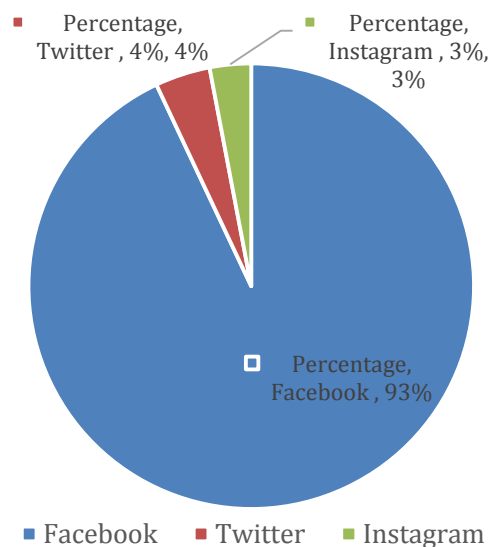


Figure (4.4) frequent distribution of the study sample according to the specialization variable

According to the table and figure (4.4) 93% they follow Facebook in using social media, only 4% are using twitter and 3% are using Instagram.

### 4.3 Hypothesis Analysis

Table (4.5) estimated table for weight means

| <b>Response</b> | <b>Mean by Weight</b> | <b>Level</b> |
|-----------------|-----------------------|--------------|
| Disagree        | 0__ 1.60              | Low          |
| Neutral         | 1.61__2.40            | Moderate     |
| Agee            | 2.41__4.0             | High         |

#### 4.3.1 First Hypothesis:

There is a statistically significant relationship between security settings and their clarity

Table (4.6) Frequency distribution of the first hypothesis statements

| <b>Statement</b>   | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|
| You can distinguish active or turned-on security features on your account. | 47         | 60        |
| You can discern the protocol used as you browse.                           | 27         | 80        |
| You can see the level of security in your account.                         | 40         | 67        |

|  |    |    |
|--|----|----|
| You can see what security settings are available to you.                   | 58 | 49 |
| Icons can be distinguished from each other.                                | 37 | 70 |
| The terms privacy and security are easy to distinguish from each other     | 92 | 15 |
| When you receive security notifications you can understand what they mean. | 36 | 71 |

According to the table (4.6): the study sample answer the statements as following:

For statement No.(1) You can distinguish active or turned-on security features on your account, 56% are responded with No and 44% are responded with Yes .

For the statement No.(2) You can discern the protocol used as you browse., 75% are responded with No , 27% are responded with Yes.

For the statement No. (3) You can see the level of security in your account, 63% are responded with No and 37% responded with Yes.

For the statement No. (4) You can see what security settings are available to you 46 % responded with No and 54% responded with Yes.

For the statement No. (5) Icons can be distinguished from each other. 65% responded with No and 35% responded with Yes.

For the statement No. (6) The terms privacy and security are easy to distinguish from each other 14% responded with No and 86% responded with Yes.

For the statement No. (7) When you receive security notifications you can understand what they mean. 66% responded with No and 34% responded with Yes.

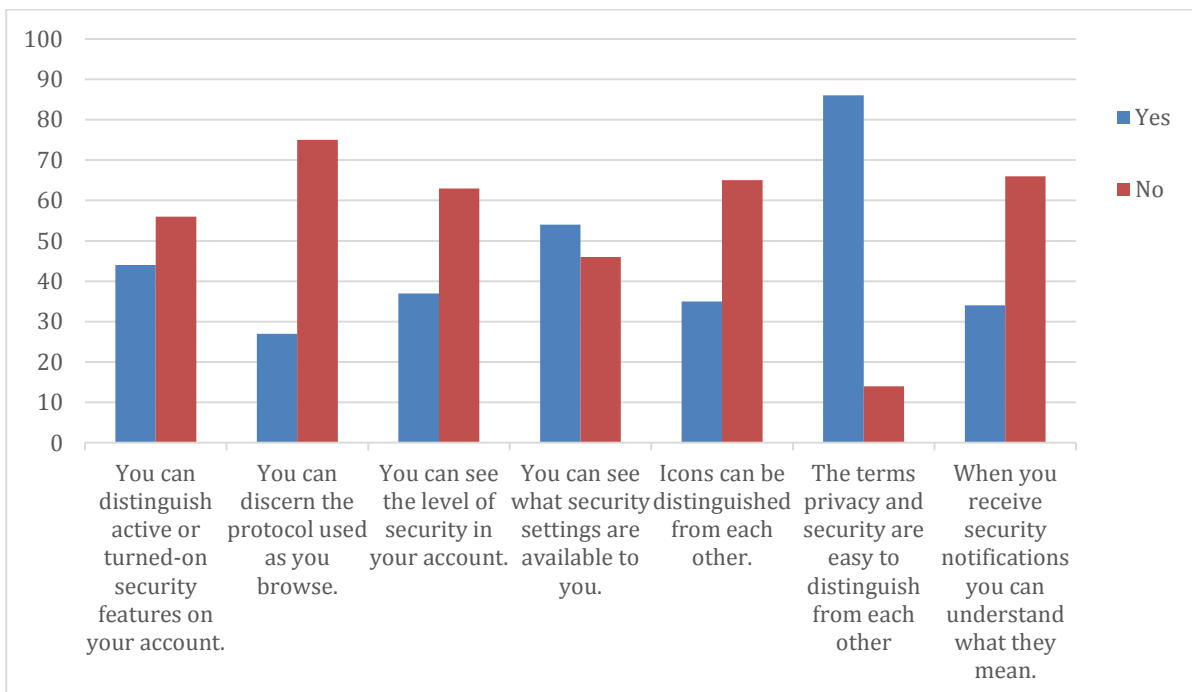


Figure (4.5) Responses about security settings and their visibility

Table (4.7) Descriptive statistics for the first hypothesis statements

| <b>Statement</b>   | <b>Yes %</b> | <b>No %</b> | <b>Mean</b> | <b>Standard Deviation</b> | <b>General direction</b> |
|--|--------------|-------------|-------------|---------------------------|--------------------------|
| You can distinguish active or turned-on security features on your account. | 44           | 56          | .44         | .499                      | Disagree                 |

|  |                 |    |     |                 |                 |
|--|-----------------|----|-----|-----------------|-----------------|
| You can discern the protocol used as you browse.                           | 25              | 75 | .25 | .436            | Disagree        |
| You can see the level of security in your account.                         | 37              | 63 | .37 | .486            | Disagree        |
| You can see what security settings are available to you.                   | 54              | 46 | .54 | .501            | Disagree        |
| Icons can be distinguished from each other.                                |                 |    |     |                 | Disagree        |
| The terms privacy and security are easy to distinguish from each other     | 35              | 65 | .35 | .478            | Disagree        |
| When you receive security notifications you can understand what they mean. | 14              | 86 | .86 | .349            | Neutral         |
| <b>General mean and standard deviation</b>                                 | <b>0.449933</b> |    |     | <b>0.308900</b> | <b>Disagree</b> |

According to the table (4.7) the responses of the study sample trend to Disagree to the statements of the first hypothesis.

#### 4.3.2 Second Hypothesis:

Table (4.8) Frequency distribution of the second hypothesis statements

| <b>Statement</b>  | <b>Freq. Percent</b> | <b>Agree</b> | <b>Neutral</b> | <b>Disagree</b> |
|---|----------------------|--------------|----------------|-----------------|
| Ease of understanding the security information presented to you | Freq.                | 91           | 0              | 16              |
|   | Percent              | 61%          | 0%             | 39%             |

|  |         |     |    |     |
|--|---------|-----|----|-----|
| Easy to get knowledge for more security                            | Freq.   | 93  | 0  | 14  |
|  | Percent | 54% | 0% | 46% |
| The privacy policy is easy to learn and understand                 | Freq.   | 77  | 0  | 92  |
|  | Percent | 28% | 0% | 72% |
| There are no health issues affecting my use of the safety settings | Freq.   | 92  | 2  | 15  |
|  | Percent | 87% | 1% | 11% |
| To reset the password, you can go to it directly                   | Freq.   | 32  | 0  | 72  |
|  | Percent | 30% | 0% | 70% |
| Famous FAQ list easy to learn from                                 | Freq.   | 35  | 0  | 72  |
|  | Percent | 68% | 0% | 32% |

According to the table (4.8): the study sample answer the statements as following:

For the statement No. (1) Ease of understanding the security information presented , 61% are agree, , 0% are neutral,39% are disagree.

For the statement No. (2) Easy to get knowledge for more security 14% 54% are agree, 0% are neutral, 46% are disagree.

For the statement No. (3) The privacy policy is easy to learn and understand, 28% are agree, 0% are neutral, 72% are disagree.

For the statement No. (4) There are no health issues affecting my use of the safety settings. 87% are agree, 1% are neutral, 11% are disagree.

For the statement No. (5) To reset the password, you can go to it directly , 68% are agree, 0% are neutral, 32% are disagree.

For the statement No. (6) Famous FAQ list easy to learn from 6% are strongly agree,30% are agree, 0% are neutral, 70% are disagree.

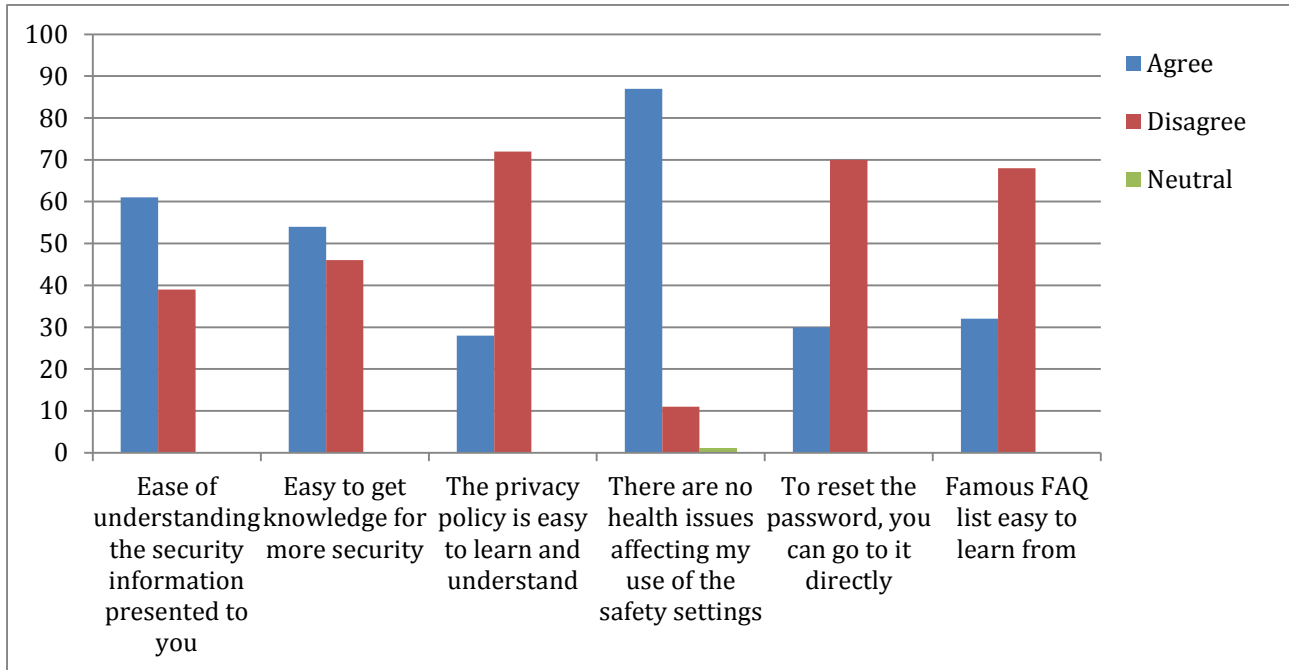


Figure (4.6) Responses about security and their learnability

Table (4.9) Descriptive statistics for the second hypothesis statements

| Statement  | Mean   | Standard Deviation | General direction |
|--|--------|--------------------|-------------------|
| Ease of understanding the security information presented to you    | 1.9720 | 1.62793            | Neutral           |
| Easy to get knowledge for more security                            | 1.7570 | 1.65313            | Neutral           |
| The privacy policy is easy to learn and understand                 | 1.1215 | 1.80518            | Neutral           |
| There are no health issues affecting my use of the safety settings | 3.5047 | 1.28396            | Agree             |
| To reset the password, you can                                     | 1.1963 | 1.84001            | Neutral           |

|  |                 |                 |                |
|--|-----------------|-----------------|----------------|
| go to it directly                          |                 |                 |                |
| Famous FAQ list easy to learn from         | 1.6636          | 1.68760         | Neutral        |
| <b>General mean and standard deviation</b> | <b>1.869159</b> | <b>1.052358</b> | <b>Neutral</b> |

According to the table (4.9) The responses of the study sample trend to Neutral to the statements of the second hypothesis.

### 4.3.3 Third Hypothesis

There is a statistically significant relationship between the use of security settings and the ease of their application

Table (4.10) Frequency distribution of the third hypothesis statements

| <b>Statement</b>   | <b>Freq. Percent</b> | <b>Agree</b> | <b>Neutral</b> | <b>Disagree</b> |
|--|----------------------|--------------|----------------|-----------------|
| Easy to set up a strong password   | Freq.                | 17           | 0              | 90              |
|  | Percent              | 16%          | 0%             | 84%             |
| Fast password setting and two-factor authentication                            | Freq.                | 14           | 0              | 93              |
|  | Percent              | 13%          | 0%             | 87%             |
| Set the password according to your preferences                                 | Freq.                | 42           | 0              | 65              |
|  | Percent              | 39%          | 0%             | %61             |
| Set up the password in the form of images instead of texts                     | Freq.                | 21           | 0              | 86              |
|  | Percent              | 20%          | 0%             | 80%             |
| To fix your account security issue, the steps you took led you to the solution | Freq.                | 15           | 0              | 92              |
|  | Percent              | 14%          | 0%             | 86%             |
| It is easy to deal with login problems to access your account                  | Freq.                | 30           | 0              | 77              |
|  | Percent              | 28%          | 0%             | 72%             |
| Security and privacy shortcuts are clear                                       | Freq.                | 30           | 0              | 77              |



|   |         |     |    |     |
|---|---------|-----|----|-----|
|   | Percent | 28% | 0% | 72% |
| The use of security in your account is related to the specifications of your device | Freq.   | 12  | 2  | 93  |
|   | Percent | 13% | 1% | 86% |

According to the table (4.10): the study sample answer the statements as following:

For the statement No. (1) Easy to set up a strong password, 16% are agree, 0% are neutral, 84% are disagree.

For the statement No. (2) Fast password setting and two-factor authentication, 13% are agree, 0% are neutral, 87% are disagree.

For the statement No. (3) Set the password according to your preferences, 39% are agree, 0% are neutral, 61% are disagree.

For the statement No. (4) Set up the password in the form of images instead of texts., 20% are agree, 0% are neutral, 80% are disagree.

For the statement No. (5) To fix your account security issue, the steps you took led you to the solution , 14% are agree, 0% are neutral, 86% are disagree.

For the statement No. (6) It is easy to deal with login problems to access your account, 28% are agree, 0% are neutral, 72% are disagree.

For the statement No. (7) Privacy shortcuts clear. 28 % are agree, 0% are neutral, 72% are disagree.

For the statement No. (8) The use of security in your account is related to the specifications of your device, 93% are agree, 1% are neutral, 6% are disagree.

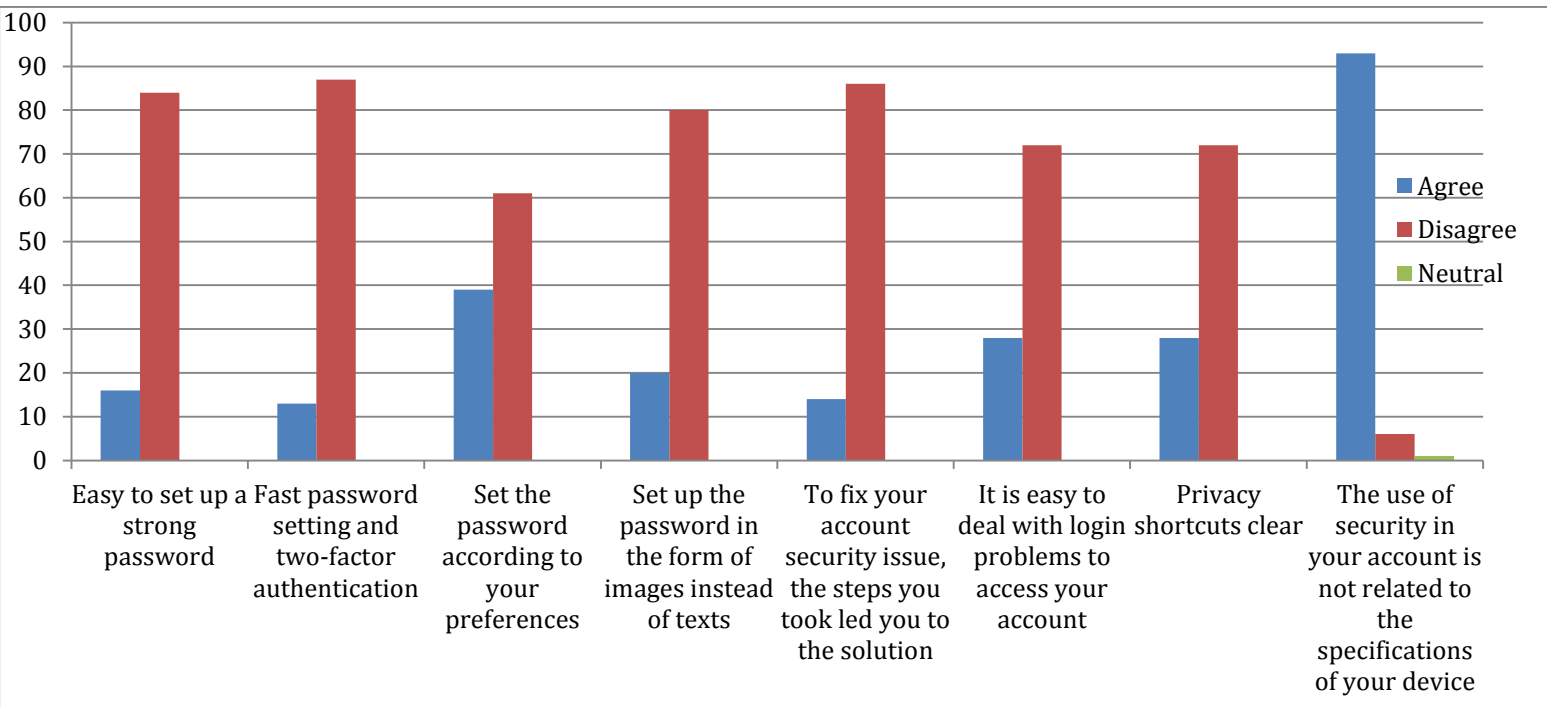


Figure (4.7) Responses about security setting and their applicability

Table (4.11) Descriptive statistics for the third hypothesis statements

| Statement  | Mean     | Standard Deviation | General direction |
|--|----------|--------------------|-------------------|
| Easy to set up a strong password   | 1.056075 | 1.365559           | Disagree          |
| Fast password setting and two-factor authentication                            | 3.299065 | 1.057007           | Agree             |
| Set the password according to your preferences                                 | 1.570093 | 1.962440           | Disagree          |
| Set up the password in the form of images instead of texts                     | 1.308411 | 1.403575           | Disagree          |
| To fix your account security issue, the steps you took led you to the solution | 0.915888 | 1.332620           | Disagree          |

|   |                 |                 |                 |
|---|-----------------|-----------------|-----------------|
| It is easy to deal with login problems to access your account                       | 1.121495        | 1.805183        | Disagree        |
| Privacy shortcuts clear   | 1.121495        | 1.805183        | Disagree        |
| The use of security in your account is related to the specifications of your device | 1.121495        | 1.805183        | Disagree        |
| <b>General mean and standard deviation</b>  | <b>1.484646</b> | <b>0.818480</b> | <b>Disagree</b> |

According to the table (4.11) the responses of the study sample tend to disagree to the statements of the third hypothesis.

#### 4.4 Chi-square Test for Hypotheses:

##### 4.4.1 First Hypothesis:

There is a statistically significant relationship between security settings are available and their clarity Table (4.12) Chi square test for the first hypotheses.

Table (4.12) Chi square test for the first hypotheses

| <b>Calculated Chi value</b> | <b>Degree of freedom</b> | <b>Significant value</b> | <b>Inference</b> |
|-----------------------------|--------------------------|--------------------------|------------------|
| 17.122338                   | 1                        | 0.001>                   | Disagree         |

According to the table (4.12) calculated Chi-Square value is (17.122338) verses Chi-Square table value (10.828) and degrees of freedom is (1) and significant value is (0.001>) and its less than significant level (0.05) so that is means there is a positive statistically significant relationship between what security settings are available and their clarity, so some users can not recognize available security settings.

#### 4.4.2 Second Hypothesis

There is a significant relationship between ease of understanding the security information and ease to get knowledge for more security

Table (4.13) Chi square test for the second hypotheses

| <b>Calculated Chi value</b> | <b>Degree of freedom</b> | <b>Significant value</b> | <b>Inference</b> |
|-----------------------------|--------------------------|--------------------------|------------------|
| 70.131583                   | 4                        | 0.001>                   | Neutral          |

According to the table (4.13) calculated Chi-Square value is (70.131583) versus Chi-Square table value (18.467) and degree of freedom is (4) and significant value is (0.001>) and its less than significant level (0.05) so that is means there is a positive statistically significant relationship between Ease of understanding the security information and ease to get knowledge for more security.

#### 4.4.3 Third Hypothesis:

There is a statistically significant relationship between the use of security settings and the ease of their application

Table (4.14) Chi square test for the third hypotheses

| <b>Calculated Chi value</b> | <b>Degree of freedom</b> | <b>Significant value</b> | <b>Inference</b> |
|-----------------------------|--------------------------|--------------------------|------------------|
| 36.220886                   | 2                        | 0.001>                   | Disagree         |

According to the table (4.13) calculated Chi-Square value is (36.220886) versus Chi-Square table value (13.816) and degree of freedom is (2) and significant value is (0.001>) and its less than significant level (0.05) so that is means there is a positive statistically significant relationship between the use of security settings and the ease of their application.

#### **4.5 Enhanced Interface for Facebook:**

The Facebook platform was chosen to suggest improving its interface because it is the most prevalent according to the sample taken. If we evaluate it according to the proposed framework, we will find that in terms of ease of use for security, it does not give the user any impression or notice about the security status or level in his account. In addition, the security settings in general are implicit and it does not have shortcuts to the most common security tasks such as changing the password or what security settings are available and activated.

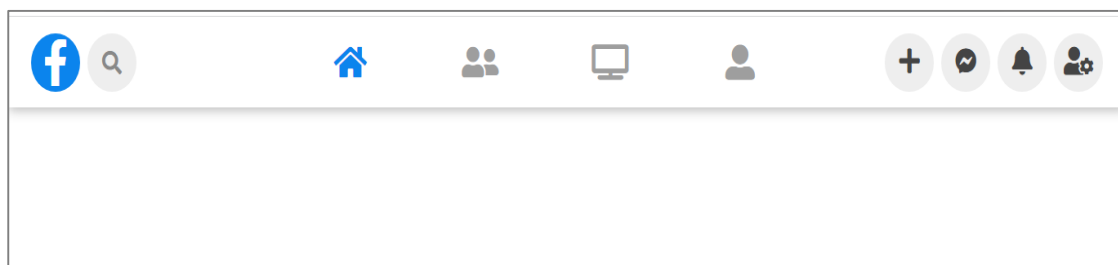


Figure (4.8) the screen of original navigation bar for Facebook:

The security icon has been added, and the icon is characterized by changing its color according to the security status of the account. In this case, it was red because it is linked to danger and was designed to blink three times to draw attention. Once you pass the cursor on it, it gives a hint called security to indicate its function.

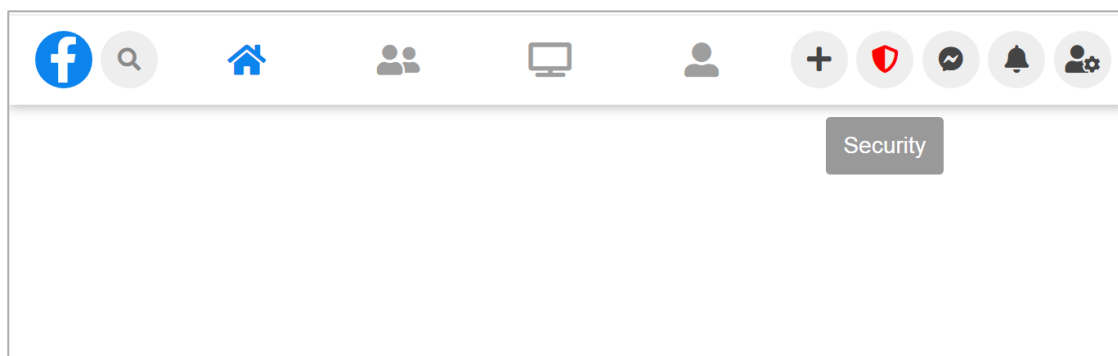


Figure (4.9) the screen of proposed navigation bar for Facebook:

In the following interface, the details for the necessary subsequent steps. On this screen, when you press the icon, a list opens containing links that are a shortcut to move user directly to adjust the settings, for example:

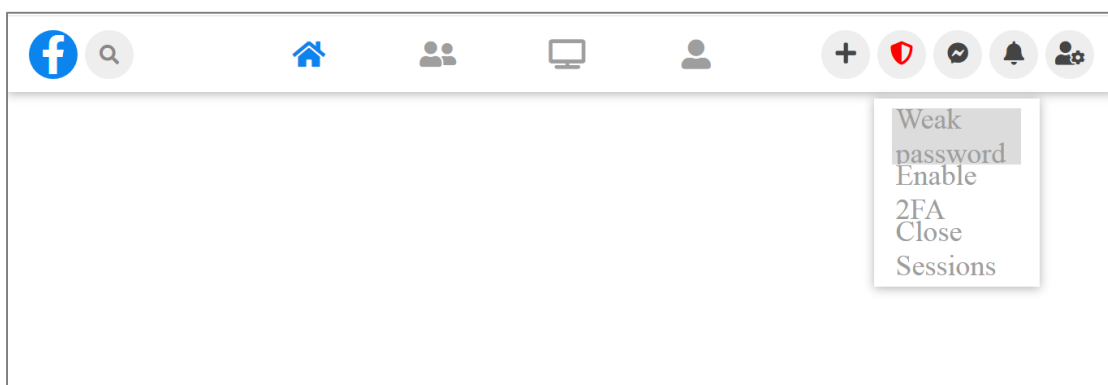


Figure (4.10) the screens of proposed navigation bar for Facebook

**CHAPTER FIVE**  
**RESULTS, RECOMMENDATIONS**

## **5.1 Conclusion**

Due to limited and non-comprehensive models available in the design of security features on the user interface on social networking sites, this study dealt with the evaluation of security using a user-based model, as it revealed problems in the ease of use of these features in terms of clarity, understanding, learning and application. The sample was collected within a specific category, it was not possible to distribute the questionnaire to the largest number due to their fear of entering into links. It was found that more than half ( 56% ) of the respondents could not distinguish the enabled/disabled and (46%) could not even recognize available security features, in addition to (75%) not being able to discern the security protocol in browsing to identify fake websites. Later, the interface of the Facebook website was designed using the model to improve the user experience with security

## **5.2 Recommendation**

The study recommends the followings:

- Study the relationship between each category with other categories and how it affects their usability
- Include a wider community for more representative results
- Suggest recognition patterns to facilitate authentication mechanisms and passwords



## 5-3 References:

- [1] A. Yeratziotis, D. Van Greunen, and D. Pottas, "A Framework for Evaluating Usable Security : The Case of Online Health Social Networks," no. Haisa, pp. 97–107, 2012.
- [2] D. Napoli, "Developing Accessible and Usable Security ( ACCUS ) Heuristics visual usage :," pp. 1–6, 2018.
- [3] S. Chiasson and R. Biddle, "Even Experts Deserve Usable Security : Design guidelines for security management systems," no. July, pp. 7–10, 2007.
- [4] C. Thirty, "Why Johnny Can ' t Encrypt," pp. 679–702, 2005.
- [5] L. Ferreira and J. Anacleto, "Usability in Solutions of Secure Email – A Tools Review," pp. 57–73, 2017.
- [6] Usable Privacy and Security for Personal Information Management, clare-marie karat, carolyn brodie, and john karat, 2006.
- [7] R. Molich and D.- Ballerup, "HEURISTIC EVALUATION," no. April, pp. 249–256, 1990.
- [8] D. Napoli, "ACCESSIBLE AND USABLE SECURITY : EXPLORING VISUALLY IMPAIRED USERS ' ONLINE SECURITY by," 2018.
- [9] "Social Media Definition." .
- [10] A. M. Kaplan and M. Haenlein, "Users of the world , unite ! The challenges and opportunities of Social Media," 2010.
- [11] Terry M. Connectivity, "Twittering Healthcare :," vol. 15, no. 6, pp. 507–510, 2009.
- [12] R. Heath, "Second Edition Edited by."
- [13] P. N. Howard and M. R. Parks, "Social Media and Political Change : Capacity , Constraint , and Consequence," pp. 1–4, 2012.
- [14] A. Russo, J. Watkins, L. Kelly, and S. Chan, "•••••," pp. 21–31.
- [15] B. K. Lewis and D. Ph, "No Title," vol. 4, no. 3, 2010.
- [16] P. Realpe-muñoz, U. Cauca, T. Granollers, J. Muñoz-arteaga, and E. B. Fernandez, "Design Process for Usable Security and Authentication Using a User-Centered Approach," 2017.
- [17] J. Nielsen, L. A. Blatt, J. Bradford, and P. Brooks, "Usability Inspection," pp. 413–414, 1994.
- [18] R. Kainda, I. Flechais, and A. W. Roscoe, "Security and Usability : Analysis and Evaluation."
- [19] "Security and human computer interfaces," vol. 22, no. 8, pp. 675–684, 2006.
- [20] I. Fléchais, "Designing Secure and Usable Systems," no. February, 2005.
- [21] "Exploring HCI ( Human Computer Interaction ) and Security in Intrusion Detection Kayhan SAYIN MSc Computer Science University of Birmingham Security and Usability."
- [22] C. Town, "13 th ANNUAL CONFERENCE ON WORLD WIDE WEB APPLICATIONS," no. January, 2011.
- [23] Y. M. Hausawi and W. H. Allen, "An Assessment Framework for Usable-Security Based on Decision Science," pp. 33–44, 2014.
- [24] J. Muñoz-arteaga, R. M. González, M. V. Martin, J. Vanderdonckt, F. Álvarez-rodriguez, and J. G. Calleros, "A Method to Design Information Security Feedback Using Patterns and HCI-Security Criteria," 2000.
- [25] S. M. Furnell, D. Katsabas, P. S. Dowland, and F. Reid, "A practical usability

- evaluation of security features in end-user applications,” vol. 232, pp. 205–216.
- [26] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, “Guidelines for Usable Cybersecurity : Past and Present.”
  - [27] I. S. Perspectives, “HUMAN COMPUTER INTERACTION : AN,” 2002.
  - [28] P. C. Realpe, C. A. Collazos, and A. Granollers, “A Set of Heuristics for Usable Security and User Authentication.”
  - [29] D. Katsabas, S. M. Furnell, and A. D. Phippen, “IT Security : A Human Computer Interaction Perspective.”
  - [30] C. A. Fidas and N. M. Avouris, “When Security Meets Usability : A User-Centric Approach on a Crossroads Priority Problem,” 2010.
  - [31] K. Yee, “User Interaction Design for Secure Systems.”
  - [32] H. Hof, “User-Centric IT Security How to Design Usable Security Mechanisms.”
  - [33] j. Raman, “security and user experience : a holistic model for CAPTCHA usability issues,” 2018.
  - [34] A. Alarifi, M. Alsaleh, and N. Alomar, “A model for evaluating the security and usability of e-banking platforms,” *Computing*, 2017.
  - [35] *Usable Privacy and Security for Personal Information Management* , by claremarie karat, carolyn brodie, and john karat
  - [36] *Research Through Design as a Method for Interaction Design Research in HCI* , (John, Jodi, Shelley 2007)
  - [37] *Towards Interface Specification and Design Guidelines to raise User Awareness of Application Security* (Rodney, Ross, 2004)
  - [38] *Measuring the Learnability of Interactive Systems Using a Petri Net Based Approach* (Andrea, Tiziana, 2018)
  - [39] *Keeping ubiquitous computing to yourself: A practical model for user control of privacy* (Blaine, Karim, Bashar, 2005).
  - [40] *International standards for HCI and usability* (Nigel, 2001)
  - [41] *Fundamentals of Inclusive HCI Design* (Julio, Luis, 2007)
  - [42] *Inclusive design and assistive technology as part of the HCI curriculum* (Helen, 2006)
  - [43] *Security and human computer interfaces* (Johnston, Eloff, Labuschagne, 2006)

# APPENDIXES

## Appendix (1)

### Questioner (English Version)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Sudan University of Science and Technology

**College of Graduate Studies**

Mr.\ .....

#### **Subject: questionnaire**

This questionnaire is part of a field study conducted by researcher to complete the requirements for obtaining a Master degree in computer science, titled (**Proposing a User-Centered Model for Evaluating the Security of Social Media**). The researcher kindly asks you to cooperate and fill out this questionnaire.

The researcher informs you that the data provided is secured and will be used for scientific research purposes only.

**Researcher**

**Frist section: Personal data:**

**1\ age:**

Less than 30 years

30 -40 years

40 – 50 years

more than 50 years

**2\ gender:**

Male

female

**3\ specialization:**

Medical and health science

engineering

Economic and management

computer science

Science and technology

arts

law

another

**4\ account in social media:**

Facebook

twitter

Instagram

## Second: Security Settings and Their Clarity

| Statement  | Yes | No |
|--|-----|----|
| You can distinguish active or turned-on security features on your account. |     |    |
| You can discern the protocol used as you browse.                           |     |    |
| You can see the level of security in your account.                         |     |    |
| You can see what security settings are available to you.                   |     |    |
| Icons can be distinguished from each other.                                |     |    |
| The terms privacy and security are easy to distinguish from each other     |     |    |
| When you receive security notifications you can understand what they mean. |     |    |

## Third: Security Settings and the Ease of Teaching Them:

| Statement  | Agree | Neutral | Disagree |
|--|-------|---------|----------|
| Ease of understanding the security information presented to you    |       |         |          |
| Easy to get knowledge for more security                            |       |         |          |
| The privacy policy is easy to learn and understand                 |       |         |          |
| There are no health issues affecting my use of the safety settings |       |         |          |
| To reset the password, you can go to it directly                   |       |         |          |
| Famous FAQ list easy to learn from                                 |       |         |          |

#### Fourth: Security Settings and Their Applications

| Statement   | Agree | Neutral | Disagree |
|---|-------|---------|----------|
| Easy to set up a strong password  |       |         |          |
| Fast password setting and two-factor authentication                                 |       |         |          |
| Set the password according to your preferences                                      |       |         |          |
| Set up the password in the form of images instead of texts                          |       |         |          |
| To fix your account security issue, the steps you took led you to the solution      |       |         |          |
| It is easy to deal with login problems to access your account                       |       |         |          |
| Privacy shortcuts clear   |       |         |          |
| The use of security in your account is related to the specifications of your device |       |         |          |

## Appendix (2)

### Questionnaire (Arabic version)

بسم الله الرحمن الرحيم

جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

#### الموضوع/ استبيان

تقوم الباحثة بإعداد بحث للحصول على درجة الماجستير بعنوان (اقتراح نموذج محوره المستخدم لتقييم أمن وسائل التواصل الاجتماعي)، وتأمل الباحثة منكم المساهمة للإجابة على هذا الاستبيان سعياً لتحقيق الهدف من هذه الدراسة. حيث أن الإجابات التي تقدمونها سوف تكون محل تقدير لما يمثله من إضافة قيمة تعكس الواقع المهني، مما ينعكس ايجابياً على اهداف هذه الدراسة، علماً بأن جميع البيانات سوف تحظى بالسرية التامة، ولن تستخدم إلا لأغراض البحث العلمي فقط.

شاكرين لسيادتكم حسن تعاملك لإتمام هذه الدراسة،،،،

الباحثة

القسم الأول: البيانات الشخصية:

الرجاء التكرم بوضع علامة (√) أمام ما يناسبك:

1/ العمر:

أقل من 20  30 وأقل من 40 سنة

31 وأقل من 40 سنة  40 سنة فأكثر

2/ النوع:

ذكر  أنثى

3/ المساق العلمي:

الطب و العلوم الصحية  لهندسة  اقتصاد وعلوم ادارية

لحاسوب وعلومه  لعلوم و التقنية  الآداب

لشريعة و القانون  أخرى

4/ هل لديك حساب على كل أو أي من المواقع التالية:



فيسبوك  تويتر  انستغرام



القسم الثاني: بيانات الدراسة:

الرجاء التكرم بوضع علامة (√) أمام مستوى الموافقة المناسب:

أولاً: إعدادات الأمان ووضوحها

| م  | العبارة   | نعم | لا |
|----|---|-----|----|
| 1. | يمكن تمييز الخصائص الأمنية النشطة أو المشغلة في حسابك   |     |    |
| 2. | يمكنك تمييز البروتوكول المستخدم أثناء تصفحك   |     |    |
| 3. | يمكنك معرفة مستوى الأمان في حسابك   |     |    |
| 4. | يمكنك معرفة الإعدادات الأمنية المتاحة لك  |     |    |
| 5. | الأيقونات  و  يمكن تمييزها عن بعضها |     |    |
| 6. | مصطلحي الخصوصية والأمان يسهل تمييزهما عن بعضهما   |     |    |
| 7. | عند تلقي إشعارات أمنية يمكنك فهم ما تعنيه   |     |    |

ثانياً: استخدام إعدادات الأمان وسهولة تعلمها:

| م  | العبارة  | أوافق | محايد | لا أوافق |
|----|--|-------|-------|----------|
| 1. | سهولة فهم المعلومات الأمنية المعروضة لك              |       |       |          |
| 2. | يسهل الحصول على المعرفة لمزيد من الأمان              |       |       |          |
| 3. | سياسة الخصوصية سهل تعلمها و فهمها                    |       |       |          |
| 4. | لا توجد مشاكل صحية تؤثر على استخدامي لإعدادات الامان |       |       |          |
| 5. | لإعادة ضبط كلمة السر يمكن الذهاب اليها مباشرة        |       |       |          |
| 6. | قائمة الأسئلة الشائعة معروفة يسهل التعلم منها        |       |       |          |

ثالثا: إعدادات الأمان و تطبيقها

| م  | العبارة   | أوافق | محايد | لا أوافق |
|----|---|-------|-------|----------|
| 8. | يسهل إعداد كلمة سر قوية                                     |       | د     |          |
| 9. | سرعة ضبط كلمة السر و المصادقة الثنائية                      |       |       |          |
| 10 | ضبط كلمة السر تراعي تفضيلاتك                                |       |       |          |
| 11 | اعداد كلمة السر في شكل صور بدلا من النصوص                   |       |       |          |
| 12 | لمعالجة مشكلة أمان حسابك الخطوات التي قمت بعملها قادتك للحل |       |       |          |
| 13 | يسهل التعامل مع مشاكل تسجيل الدخول للوصول الى حسابك         |       |       |          |
| 14 | اختصارات الامان الخصوصية واضحة                              |       |       |          |
| 15 | استخدام الأمان في حسابك يتعلق بمواصفات جهازك                |       |       |          |

## Appendix (3)

### The Code Used for Enhanced Facebook Navigation Bar

#### Consider Proposed Model

##### HTML file:

```
<header>
  <linkrel="stylesheet"
href="https://use.fontawesome.com/releases/v5.8.2/css/all.css"><link href = "style.css"
rel = "stylesheet" type = "text/css" >
<nav>
<ul> <li> <a href="#" id="fb"> <i class = "fab fa-facebook-f"> </i> </a> </li>
<li> <button id="search_btn" class="tooltip" data-tooltip="Search"> <i class="fas fa-
search"></i> </button> </li>
<li id="space2"></li>
<li> <a class="tooltip active" data-tooltip="Home" href="#" id="home"> <i class="fas
fa-home "></i> </a> </li>
<li> <a class="tooltip" data-tooltip="Group" href="#" id="group"> <i class="fas fa-
user-friends"></i> </a></li>
<li> <a class="tooltip" data-tooltip="Watch" href="#" id="tv"> <i class="fas fa-tv
"></i> </a> </li>
<li> <a class="tooltip" data-tooltip="Friend" href="#" id="friend"> <i class="fas fa-
user-alt "></i> </a> </li>
<li id="space1"></li>
<li> <button class="tooltip" data-tooltip="Add" id="btn_plus"><i class="fas fa-plus
"></i></button> </li>
<li> <button class="tooltip" data-tooltip="Security" id="btn_security"><i class="fas fa-
shield-alt blink" style = "color:red" ></i></button>
<ul class = "dropdown">
```

```

<li><a href="#">Weak password </a></li>
<li><a href="#">Enable 2FA</a></li>
<li><a href="#">Close sessions</a></li></ul></li>
<li> <button class="tooltip" data-tooltip="Message" id="btn_msg"><i class="fab fa-
facebook-messenger  "></i></button></li>
<li> <button class="tooltip" data-tooltip="Notification" id="btn_bell"> <i class="fas fa-
bell"></i></button></li>
<li> <button class="tooltip" data-tooltip="Profile" id="btn_profile"><i class="fas fa-
user-cog "></i></button> </li></ul>
</nav></header>

```

**CSS file:**

|   |  |
|---|--|
| <pre> *{   box-sizing: border-box; } :root{   --btn-width-100: 100px; } body{   margin: 0;   padding: 0; } nav{   margin: 0;   padding: 0; } nav ul {   margin: 0;   padding: 8px 15px;   list-style: none;   display: flex;   box-shadow: 0 1px 8px   rgba(0,0,0,0.3); } nav ul li {   padding: 3px; } nav ul li a{ </pre> | <pre> display: inline-block; text-decoration: none; } nav ul li #fb{   background: #0B84ED;   color: #fff;   width: 40px;   height: 40px;   border-radius: 50%;   display: flex;   justify-content: center;   align-items: center;   font-size: 2rem; } nav ul li #search_btn{   border: none;   outline: none;   background: rgba(0, 0, 0, 0.068);   padding: 8px;   color: #888;   width: 40px;   height: 40px;   font-size: 1rem;   border-radius: 50%;   cursor: pointer; } </pre> |
|---|--|

```

nav ul li#space1{
flex: 1;
}
nav ul li#space2{
flex: 2;
}
nav ul li a{
height: 40px;
width: var(--btn-width-100);
font-size: 1.5rem;
display: flex;
justify-content: center;
align-items: center;
color: rgb(158, 158, 158);
transition: .5s
}
nav ul li #btn_plus,
nav ul li #btn_security,
nav ul li #btn_msg,
nav ul li #btn_bell,
nav ul li #btn_profile{
height: 40px;
width: 40px;
display: flex;
justify-content: center;
align-items: center;
font-size: 1.2rem;
color: #444;
background: rgba(0, 0, 0, 0.068);
border: none;
outline: none;
border-radius: 50%;
cursor: pointer;
}
nav ul li:hover #home,
nav ul li:hover #group,
nav ul li:hover #tv,
nav ul li:hover #friend{
background: rgba(0, 0, 0, 0.138);
color: #444;
border-radius: 5px;
}
.active{

```

```

color: #0B84ED!important;
}
.tooltip{
position: relative;
}
.tooltip::after{
content: attr(data-tooltip);
height: 30px;
background: rgba(0,0,0,0.4);
color: #fff;
font-size: 1rem;
text-align: center;
position: absolute;
bottom: -150%;
padding: 5px 12px;
line-height: 30px;
border-radius: 3px;
opacity: 0;
transition: .3s;
pointer-events: none;
user-select: none;
}
.tooltip:hover::after{
opacity: 1;
}
nav ul li #btn_profile::after{
margin-left: -20px;
}
@media screen and (max-width:
700px){
nav ul li#space1,
nav ul li#space2{
display: none;
}
nav ul{
min-width: 600px;
padding: 8px 12px;
justify-content: space-between;
}
:root{
--btn-width-100: 60px;
}
}

```

```

.blink {
animation: blink 1s ;
animation-iteration-count: 5;
}
@keyframes blink {
0% {
opacity: 1;
}
50% {
opacity: 0;
}
100% {
opacity: 1;
}
}
.drop-menu{
position: absolute;
background: #242526;
width: 180px;
line-height: 45px;
top: 85px;
opacity: 0;
visibility: hidden;
box-shadow: 0 6px 10px
rgba(0,0,0,0.15);
}
.drop-menu li a{
width: 100%;
display: block;
padding: 0 0 0 15px;
font-weight: 400;
border-radius: 0px;
}
.drop-menu li{
margin: 0;
}
.drop-menu li a{
border-radius: 5px;
font-size: 18px;
}
#showDrop:checked ~ .drop-
menu{
max-height: 100%;

```

```

}
a {
text-decoration: none;
}
nav {
font-family: default;
}
ul {
background: #ffffff;
list-style: none;
margin: 0;
padding-left: 0;
}
li {
color: #fff;
background: #ffffff;
display: block;
float: left;
padding: 1rem;
position: relative;
text-decoration: none;
transition-duration: 0.5s;
}
li a {
color: #ffffff;
}
li:hover,
li:focus-within {
background: #ffffff;
cursor: pointer;
}
li:focus-within a {
outline: none;
}
ul li ul {
background: #ffffff;
visibility: hidden;
opacity: 0;
min-width: 5rem;
position: absolute;
transition: all 0.5s ease;
margin-top: 1rem;
left: 0;

```

```
display: none;
display: inline-block;
}
ul li:hover > ul,
ul li:focus-within > ul,
ul li ul:hover,
ul li ul:focus {
visibility: visible;
opacity: 1;
display: block;
```

```
}
ul li ul li {
clear: both;
width: 100%;
}
ul li ul li:hover,
ul li ul li:focus-within {
background: #dcdcdc;
cursor: pointer;
}
```