University Institute of Lisbon

Information Science and Technology Department

Methodology for discussing the impacts of Two-factor authentication in user activities

Indira Barreto Pina Sanches

A Dissertation presented in partial fulfillment of the Requirements for the Degree of

Master in Computer Engineering

Supervisor:

Doctor Maria Pinto-Albuquerque, Assistant Professor

ISCTE-IUL

October, 2017

Acknowledgements

I would like to thank all of the people who turned this research possible to be made.

First of all, I would like to thank my supervisor prof. Maria Pinto-Albuquerque, for her supervision, support, availability, and dedication to this research.

I would like to thank all of the people who were part of the experimentation. Students of ISCTE-IUL and my friends and colleagues in Cabo Verde, Brazil, the United Kingdom and the United States of America.

I would like to thank my parents Hélio and Ivete, my inspirations, who always made their best to turn my dreams come true. I am deeply grateful for their love, support and patient. Without their help, the accomplishment of this research would not be possible, and for that I am very grateful.

I would like to thank my sister Ariana and my bestfriend Samir who were always here for me during this research helping me in all of the stages of it. Thank you for the love and support.

I would like to thank my friends, in particular Carlisa, Indra, Nadine and Eliane who helped me during the accomplishment of the experiments conducted. To all of you, I am deeply grateful for your love and support.

Resumo

A proteção dos sistemas de informação é muito importante para as organizações. Uma medida de segurança adotada pelas organizações é a implementação de políticas de segurança. Contudo, se estas políticas não levam em consideração as atividades dos utilizadores estes podem comprometer a segurança da informação.

O objetivo desta investigação é propor uma framework para discutir os impactos das políticas de segurança nas atividades dos utilizadores e aplicar esta framework geral a uma política de segurança, autenticação de dois fatores, de modo a perceber o impacto da sua adoção nas atividades dos utilizadores.

Nesta dissertação propomos uma abordagem onde os utilizadores têm a possibilidade de escolher as funcionalidades de sistemas de E-learning e homebanking que devem conter 2FA.

A metodologia apresentada para discutir o impacto do 2FA nas atividades dos utilizadores provou ser eficaz uma vez que, para além de ter aumentado o conhecimento dos utilizadores neste tópico, forneceu descobertas relacionadas com:

- Adoção do 2FA nos sistemas de E-learning e homebanking;
- Funcionalidades que os utilizadores consideram que deve conter 2FA;
- Vantagens e desvantagens do 2FA do ponto de vista dos utilizadores.

Uma contribuição chave desta dissertação para o estado da arte é que fornece contribuições importantes da utilização do 2FA em sistemas de E-learning e homebanking; e apresenta uma abordagem que confere aos utilizadores a possibilidade de escolherem as funcionalidades que devem conter 2FA, o que até à data não foi proposto.

Palavras-chave: Segurança de tecnologias de informação, políticas de segurança, factor humano na segurança de informação, 2FA, E-learning, Homebanking.

Abstract

The protection of information systems is very important to organizations. A security measure adopted by organizations is the implementation of security policies. However, if these security policies do not take into consideration user activities they can compromise the security of information.

The aim of this research is to propose a framework for discussing the impacts of security policies in user activities and apply the general framework to a specific IT security policy, two-factor authentication, in order to understand the impacts of its adoption in user experience.

This dissertation proposes an approach where users have the possibility of choosing the functionalities of E-learning and homebanking systems that should have 2FA applied to it.

Our methodology for discussing the impacts of 2FA in user activities proved to be effective since, besides increasing users knowledge on 2FA and its related concepts, it also provided findings on:

- 2FA adoption in E-learning and homebanking systems;
- Functionalities that users would want to apply 2FA and 1FA;
- 2FA advantages and disadvantages perceived by users.

A key contribution of this dissertation to the state of art is that it provides important contributions to 2FA studies on E-learning and homebanking systems and presents an approach where users have the possibility of choosing the functionalities that they would rather have 2FA on it, that hasn't been proposed up to date.

Keywords: Information technology security, Security policies decisions, Human factors in security, 2FA, E-learning, Homebanking.

Table of contents

List of figures

List of tables

List of graphs

Introduction

1.1. Introduction

Information security policies are essential to protect information from the threats they are exposed to nowadays (Knapp, Morris, Marshall, Byrd, & Sykes, 2009). However, security policies that are based only on technological approaches usually hinder the adaptation to those policies. It is very important to take into consideration the human factor in information security policies (Metalidou et al., 2014). Users play an important role in information security since they are the ones using/that will use the security policies applied (Koh, Ruighaver, Maynard, & Ahmad, 2005).

In this dissertation we propose a framework for analyzing IT security policies in terms of usability and security enabling the discussion of their impacts in user activities. This analysis will be made in order to help recommend the most appropriate security policy to adopt or and/or justify the choice made.

We applied the general framework to a specific IT security policy called two-factor authentication (2FA). 2FA is a security policy that provides a stronger authentication by asking for more than one factor during the authentication process (Tsymzhitov, Zudilova, & Voitiuk, 2016). Although it is still not used by many people/organizations it has been gaining popularity with the increasing number of accounts and information being hacked (De Cristofaro, Du, Freudiger, & Norcie, 2013).

The focus of this dissertation is on analyzing the impacts of a specific IT security policy, 2FA, in terms of usability and security in users activity. Moreover, we propose an approach where users have the possibility of choosing which functionalities of homebanking and E-learning systems should have this mechanism applied. By giving users this possibility we expect to introduce the "human factor" in security policies as explored by many researches. That is, to take into consideration their activities when creating and implementing security policies.

This chapter presents the motivation of this research and the problem of security policies that do not take into consideration the human factor in information security. It then defines the scope of this research and gives an overview of the problem that motivated the appearance of 2FA and its concept.

The chapter then presents the aim, objective and research question of this research. At last, it describes our approach for discussing/analyzing the impacts of security policies in user activities and gives a brief description of the experimentation planning.

1.2. Motivation and problem

In a new era where we face problems such as cybercrime, information security stands as a crucial aspect in the protection of data confidentiality, availability and integrity.

Information is one of the most valuable assets any organization can have. For this reason, it is essential to protect it from the variety of threats we face nowadays. In this context, security policies aim to ensure information security and avoid problems such as confidential information theft, use of information for illegal purposes, among others.

Security policies define a set of standards/rules that allow information security management in an organization and they are essential for reducing the impacts caused by lack of security. The cybersecurity community is aware of the importance of the human aspect in the establishment of effective security policies. Palo Alto Networks (a big cybersecurity company) reflects this awareness in its Information Technology (IT) Security Policy, "An information Technology (IT) Security Policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources. Effective IT Security Policy is a model of the organization's culture, in which rules and procedures are driven from its employees approach to their information and work" (Palo Alto Networks., n.d.).

Each organization must adapt security policies to their own scenario and every employee that has access to the company's information must follow these policies. When implementing information security policies in an organization factors such as the cost associated with the implementation of these mechanisms, their impact in user activities and the usability of the mechanism must be considered.

We can help managers make decisions regarding IT security if we enable them to understand the importance of security policies and discuss with other professionals (e.g security engineers, users/employees) about the variety of aspects involved (costs, usability, interference at work, etc) and their impacts. It is also relevant to communicate to users the importance of information

security in order to facilitate their adaptation to the security policies implemented in the organization.

User activities may be affected by the implementation of security policies. These security policies can be very demanding for users making the adaptation period longer. Furthermore, when security policies do not take into consideration user activities the probability of finding "work-arounds" increases. This in turn, decreases IT security (Ang et al., 2007).

In this dissertation, we propose an approach for discussing the impacts of the IT security policy 2FA in user activities in terms of security and usability. In the beginning of this research, we proposed a general framework for analyzing and discussing the impacts of security policies in user activities. In this research, we applied the general framework to a specific security policy, 2FA, and we analyzed its impact in terms of security and usability in user activities.

1.3. Scope of the dissertation

The focus of this dissertation is on discussing the impacts of the adoption of the IT security policy, 2FA, in user activities in terms of security and usability.
Our goal is to try to find a balance between security and usability. We want to have the appropriate security for the usage context of a certain functionality of a system, but the minimum possible interference in user activities.

With this research, we want to understand if increasing security of certain functionalities of systems bothers/disturbs users activities and if they realize the importance of higher security levels in some functionalities of internet services.

In addition, we propose an approach that we believe can improve user experience with 2FA decreasing the negative impact it might have in user activities and thus increase user adherence to 2FA when it is appropriated. We intend to give users the possibility to choose which functionalities should contain 2FA on it.
This research will focus on applying 2FA to access some functionalities of a given internet service and after a successful login.

We also want to understand if in case there are functionalities where is mandatory to have 2FA on it users will still prefer to have access to that functionality using 2FA or not having internet access to that functionality.

We plan to study user adherence to 2FA in two different contexts: in a university student web portal and in a homebanking system. We also intend to study/evaluate the knowledge that the target audience has about 2FA and [2]1FA concepts and if possible, increase their understanding on this topic.

1.4. 2FA Mechanism

1.4.1. Problem

Many of the services we have access through the internet nowadays involve the process of confirming the identity of users. That is, to prove that users are who they say they are. This process is called authentication. According to SANS Institute, "Authentication is done by using something you know (such as your password), something you have (such as your smartphone) or something unique to you (such as retinal scan or fingerprint)".

The most common method used for authentication is using just a username and a password. This type of authentication is called 1FA (Tsymzhitov et al., 2016).

This authentication method presents some security gaps. Nowadays, there are many ways to discover users passwords and consequently having access to user's internet accounts. Brute force, key loggers and malwares are some popular techniques for cracking passwords. This means that, if attackers discover the password, they can instantly have access to users information. The scenario gets worse if users use the same password for multiple accounts (Tsymzhitov et al., 2016).

There are different 2FA technologies that can be used by services. The most common ones are: smartphone applications, codes received via SMS/Email and codes generated by a security token (De Cristofaro et al., 2013).

[2] From this point in the dissertation the abbreviation 1FA will be used to mean single-factor authentication.

1.4.2. Concept

In order to ensure a stronger authentication, it is necessary to use more than a single-factor. 2FA is an authentication process that uses two verification methods in order to prove that users are who they say they are.
With 2FA, users will still have to introduce their email and password, but if the credentials are successfully validated they will not have direct access to their account. They will have to introduce a second-factor. With this authentication method, even if attackers find users password they won't have access to users account if they don't have the second-factor (Tsymzhitov et al., 2016).

This authentication method is usually implemented in enterprises, online banking and government but over the years it is gaining popularity with the increasing number of accounts and passwords hacked (De Cristofaro, Du, Freudiger, & Norcie, 2013).

Although 2FA adds an extra layer of security by asking for more than one factor, some authors argue that this mechanism schemes can be circumvented (Adham, Azodi, Desmedt, & Karaolis, 2013).

1.5. Aim, objectives and research question

The aim of this research is to propose a framework for discussing the impacts of security policies in user activities and apply the general framework to a specific IT security policy (2FA) in order to understand the impacts of its adoption in user experience and to improve security awareness in the human resources of an organization.

This approach will include an experimentation with users. The following objectives are also pursued by conducting the experimentation:

1. Propose an approach to study the usability and security of 2FA in user experience in order to increase user awareness of internet security and experience with services provided by the internet.

1.a. Analyze user awareness and acceptance of security advantages and disadvantages of 1FA and 2FA.

1.b. Increase user awareness of internet security.

1.c. Increase user experience with the services provided by the internet, including its security.

2. Analyze the implementation of 2FA in a university student web portal and in an homebanking system.
3. Understand user preferences for deciding between having a functionality with mandatory 2FA on it, or not having internet access to that functionality.

The research questions are:

1. How does 2FA affect user activities in terms of usability and security?

2. Is it a good approach to provide users with the possibility of deciding between:

a. 1FA or 2FA for a certain functionality of a system;

b. 2FA or not having internet access to the functionality of the system;

in order to minimize the negative impacts of its adoption in user activities and to increase user experience and user acceptance regarding security aspects?

3. What is the knowledge that the users have about the 2FA and 1FA concepts?

1.6. Proposed approach

In this dissertation, we propose a framework for discussing/analyzing the impacts of security policies in user activities. With this framework, we want to demonstrate/explore/discuss the impacts (advantages/disadvantages/consequences) of security policies in user activities. We plan to apply the framework proposed to a specific IT security policy, 2FA, and discuss the impacts of its adoption in terms of security and usability.

Besides that, we also propose an approach where users have the opportunity of choosing which system's functionality should have 2FA on it.

We consider that by giving them this opportunity they will have better experiences while using an internet service because they'll have the chance to apply 2FA only in data/functionalities that they consider important (should not be disclosed to others). We hypothesize that by this way user adherence to 2FA will increase.

We consider that by giving users the opportunity to apply 2FA in functionalities they consider important organizations will be trying to ensure both the security of their services but also the service's usability.
In a user's perspective, they will have the chance to protect only information that is confidential decreasing the burthen of using a system that does not meet user's necessity.
According to Hiltgen et al. (2006), "Providing an appropriate balance between convenience and security is a current concern for the industry".

1.6.1. Experimentation planning

This approach will include an experimentation with users. There will be made two types of experimentations: face-to-face and long-distance experimentations. It will have as target audience college students.

The experimentation will include a presentation of 2FA, a Java program that users can test to understand how 2FA works and three questionnaires that users will have to respond to: an introductory questionnaire, a questionnaire about E-learning system and a questionnaire about homebanking system.

1.7. Outline of the dissertation

This dissertation is structured in 6 chapters that present the different phases of this research.

Chapter 1 introduces the research conducted and gives an overall view of the background, importance and motivation to this study.

Chapter 2 describes the related work on information security and 2FA. In this chapter, we present a series of studies on users perception of information security, the importance of the human factor in information security, security policies in organizations, and studies about the specific security policy that will be analyzed in this research, 2FA.

Chapter 3 is dedicated to the proposed approach. First, we present the general framework created, and then we describe how the general framework motivated the development of the specific approach that focuses on analyzing the impact of 2FA in user activities.

Chapter 4 describes the evaluation for this research. It presents the goals of the evaluation and the methodology applied to the research. The chapter also presents the activities of the experimentations that were conducted and a description of each one of them. It then describes the experimentation in action.
The chapter concludes with the presentation of the quantitative and qualitative results.

Chapter 5 is dedicated to the discussion of results. In this chapter, we present an analysis of the results and the main findings of this research.

At last, chapter 6 presents the conclusions of this study and proposals for future work.

2. Literature review

2.1. Introduction

This chapter describes the state of the art of information security policies and two-factor authentication (2FA) researches.

The chapter starts by introducing the concept of users perception of information security and the studies conducted about information security risk analysis. It then describes the human factor in information security policy as an important factor to take into consideration when adopting and implementing security policies. This topic also describes some issues related to password policies such as: studies that explore what makes users compromise their passwords, the problems with implementing rigid password policies, and some remedial measures that can be taken to decrease the negative impact caused by lack of password security.

It then introduces some research conducted on 2FA such as studies on its adoption, comparisons between 2FA technologies and usability/security studies on E-learning and homebanking systems.

The chapter ends with a description of the contribution of the studies for our research.

2.2. Users perception of information security

The security of information systems is a major problem faced by users and organizations. It is essential to apply information security policies in order to manage the security of information systems. However, many aspects have to be considered when formulating, implementing and adopting a successful security policy (Karyda, Kiountouzis, & Kokolakis, 2005).

Information security solutions based only on technological approaches are not sufficient to protect data. Factors such as the culture of the organization, the organization structure and user satisfaction with previous policies have to be considered because these IT security solutions will be used by the employees of the organizations. User satisfaction is used to measure how successful the information system will be (Montesdioca & Maçada, 2015).

Ang et al. (2007) have proposed a “House of Security”, which is a security assessment model that considers eight aspects regarding security: Vulnerability, Accessibility, Confidentiality, Technology Resources for Security, Financial Resources for Security, Business Strategy for Security, Security Policy and Procedures, and Security Culture. This project’s main objective is to identify similarities and differences within and between different organizations regarding the perceptions of security by different members of an organization. A survey was conducted and the respondents were asked to rate some statements about their perception of security. The preliminary results found out that different people in an organization have different perceptions and awareness regarding their own company’s security (Ang et al., 2007).

Another survey was conducted and its main objective was to develop a model to measure user satisfaction with information security policies. The results demonstrate that users understand what the benefits of information security practices are. However, there is a negative relation between information security practices and user satisfaction. These results are important because they validate the need to develop security policies that facilitate the use of information systems. The model developed can be applied to specific organizations to identify gaps and contribute to the implementation of security policies that are aligned with user/employee and organization’s needs (Montesdioca & Maçada, 2015).

2.3. Information Security Risk analysis

Every organization has assets that are considered more important than others. Therefore, the complexity of information security policy systems may vary depending on the type of data we want to protect (Magaya & Clarke, 2012).

The first thing a business needs to know in order to improve their information security is what resources need to be protected. It is necessary to evaluate the risks associated and determine which risks can be consider acceptable (Storms, 2004).

Magaya & Clarke (2012) argue that “In the Enterprise world, the most effective tool for ensuring organizations are well protected is risk management. It is an approach that ensures that a commensurate approach to protection is provided – providing more security to assets that are more valuable than others.” However, these tools require the use of expertise and may be too expensive for home users.

A risk analysis consists in an evaluation of the vulnerabilities of a system and the threats it might be exposed to. This is an indispensable process in a risk management program. The process contributes for the establishment of protective security measures for the systems/information of the organization (Jenkins, 1998).

Magaya & Clarke (2012) have proposed a web-based risk analysis tool for home users, Webra tool, that is user friendly and does not require prior knowledge of security. This tool aims to improve user's security posture by analyzing key assets and provide an overall risk rating for these assets. Webra tool has four main processes: asset selection, behavioural practice, control ranking and output/recommendations.

In the asset selection process users select their assets, services that are used and controls currently implemented. In behavioral practice users respond a set of questions about their use of systems. The system analyzes the controls that are missing and determines the risk level based on a control priority ranking system, this corresponds to the control ranking process. The last process corresponds to the generation of output/recommendations. In this process, the tool provides an overall risk rating for the assets that were selected in the asset selection process and recommends missing controls that are essential to mitigate the risks. The prototype was evaluated, and the results indicate that most of the users found Webra tool easy to use and could be used with minimum security knowledge. Users also felt that the tool provided the necessary assistance to select and implement the recommending controls.

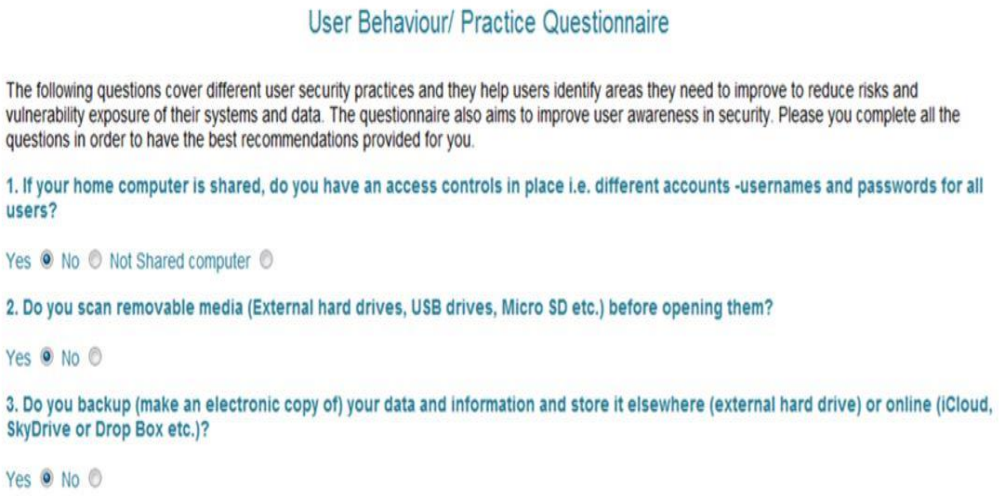


Figure 1: Webra tool - Behavioural questionnaire – Source (Magaya & Clarke, 2012)

Critical Controls	WEBRA Controls	Priority
Inventory of Authorized and Unauthorized Devices	Identify the assets the user has done by the tool (Stage 1 WEBRA)	RA tool
Secure Configurations for Hardware and Software on Laptops, Workstations, and mobile devices	Secure configuration of security software and system settings.	High
Continuous Vulnerability Assessment and Remediation	Patches and updates	High
Malware Defences	Anti- Virus, Anti-Spyware	High
Controlled Use of Administrative Privileges	Passwords	High
Application Software Security	Encryption	Moderate
Data Recovery Capability	Backups	Moderate
Secure Configurations for Network Devices such as Firewalls, Routers incl. wireless, and Switches	Firewalls	Moderate
Boundary Defence	Physical security, case, pouch	Moderate
Controlled Access Based on the Need to Know	User Accounts for different users	Low
Account Monitoring and Control	Biometrics	Low

Table 1: Webra tool - Asset priority list - Source (Magaya & Clarke, 2012)

2.4. The Human factor in information security

Employees of an organization are often the weak link when regarding the protection of information. The human factor in information security has a major impact on the success or failure of information systems (Metalidou et al., 2014). However, information security is a human factor problem that remains unaddressed (Schultz, 2005). This may be caused by the fact that employees are faced constantly with rigid security policies and complex information security system.

Information security policies and standards defined by organizations are not implemented only by computers. People are responsible for configuring and acquiring systems among other functions. It is important to pay attention both to people and to technology (Hinson, 2014).

Metalidou et al. (2014) have proposed a framework to examine the correlation of human factors with the lack of information security awareness. The objective of this study was to identify the human weaknesses that caused security issues and suggest ways to overcome them. The authors categorize the factors that affect security of computers into two categories: human factor and organizational factor. This study focusses on five human factors that were determine by Badie & Lashkari (2012) and are the following: lack of motivation, lack of awareness, belief,

behavior, inadequate use of technology and computer security risks. These human factors have major implications in users behavior and are the key to mitigate security threats that are caused by humans. It is very important for organizations to cultivate an environment where positive security behaviors by users are valued. Security policies need to be comprehensible and flexible because when technology fails users/employees depend on the services provided by organization to overcome these fails (Orshesky, 2003)

Hinson (2014) argues that there is a great need to tackle the human factor in information security. In order to improve information security, it is needed more than just improving technological procedures. It is needed to improve both aspects since they play important roles in this field.

Several studies have been made to understand the impact of security policies in user activities as well as studies about the experiences users go through when using passwords. The final goal of these studies is to find ways to raise awareness of the dangers associated with weak security policies but also trying to adapt these policies to user's needs.

Adams and Sasse (1999), address this problem studying what makes users compromise computer security systems as well as remedial measures to be adopted. The study demonstrates that many users do not create strong and secure passwords because they are not conscious of the problems that can be caused by lack of password security. Many users create multiple passwords for different services. In this scenario, users have to memorize multiple passwords, which can become more difficult to remember if the number of passwords continue to increase. Furthermore, some passwords may be used with less frequency then others and so, after long periods of inactivity of an account, users may forget their authentication credentials. As a solution to this problem, users usually write down their passwords (in paper or digital format). However, in these cases passwords may become vulnerable and can be captured by hackers or users may forget the place where the password was kept.

In this situation, it can be considered the use of Single Sign On (SSO) mechanism as a security policy. This mechanism allows users to have access to multiple services using one set of login credentials. Users only have to memorize one single password, the one that allows having access to multiple services. This will have significant impact on helpdesks requests since the probability of users forgetting their passwords will decrease.

It is becoming more difficult to create passwords that correspond to security policies implemented in an organization. This has to do with the fact that security policies have become

more rigid in order to ensure the creation of stronger passwords, which reduce the chances of passwords being captured. On one hand, security managers argue that if users understood the dangers associated with lack of security policies, they would behave differently. On the other hand, users argue that if security managers understood the true costs for users and the organization, perhaps they would have set security policies differently (Inglesant and Sasse , 2010).

Another scenario being studied is the experience of password reset policies. The aim of this study is to analyze the impact of password reset policies in universities upon users experience and productivity.

Password reset in universities usually take place after long periods of inactivity of an account (e.g Summer, Easter or Christmas break). Students understand the need for password reset periodically, however, they find the process boring and tiring. As a solution to this inconvenience students tend to create as the new password the previous password with little changes in order to be easier to remember. Training students/users to create secure and easy to remember passwords is a major challenge in order to decrease helpdesk requests (Parkin, Driss, Krol, & Angela Sasse, 2016).

The way security policies are implemented have a major impact in the experiences faced by users in the scenarios previously referred. Therefore, to be successful security policies have to provoke positive user experiences.

2.5. Impact of security policies in organizations

A case study was developed to analyze the implementation of security policies in two organizations (non-governmental and governmental organization) and a framework was developed with the aspects regarding the implementation of security policies. The results indicate that the implementation of information security policies is affected by the different contexts within which they take place, as well as the cultural elements in an organization. The case study also showed that, the security officer has an important role during the formulation and implementation of security policies. A motivated and qualified security officer can lead the process of implementation and adoption and assure successful security policies. It is also

important to implement security policies that meet users professional goals in order to increase their productivity (Karyda et al., 2005).

In order to determine the success of security policies it is necessary to evaluate them. Before evaluating security policies, the documentation of the development process will have to be created. This document may allow the evaluation to identify if improvements have been made in the policy development process. Nowadays, security policies evaluation only concentrates on the policy and does not consider other problems in the organization that may have contributed for the policy to be developed. There may have been political pressures to implement a policy forcing users to adapt to those policies without any consultation. Having documentation available enables access to the detailed method used in policy development and can help determine if the policy covers the issues identified within development. The criteria used for evaluating security policies may vary depending on the context of the organization. This occurs because of the subjective nature of developing a security policy and the context in which it is being implemented (Maynard & Ruighaver, 1999).

2.6. 2FA as an IT security policy

2.6.1. Quantifying 2FA's adoption

A security policy that has being gaining popularity nowadays and that is going to be analyzed in this dissertation is 2FA. Google, Facebook and Yahoo are examples of service providers that adopted 2FA in order to protect sensitive and personal information. Although 2FA has been gaining popularity due to the increase of passwords being hacked, rates about their adoption are still low (De Cristofaro et al., 2013).

With the increasing number of organizations adopting this authentication method it is important to understand who is willing to implement 2FA in their organization. Petsas et al. (2015) made a research where they tried to quantify the adoption of 2FA on Google. This research chose to study Google's account since this organization is probably the largest existing service provider. The authors examined over 100.000 accounts and concluded that 2FA has only been adopted by 6,4% of users. This brings the question that remains: Can this mechanism be adopted by the majority of users?

Other studies showed that in the business context 17% of enterprises adopted 2FA (Humphries, 2015).

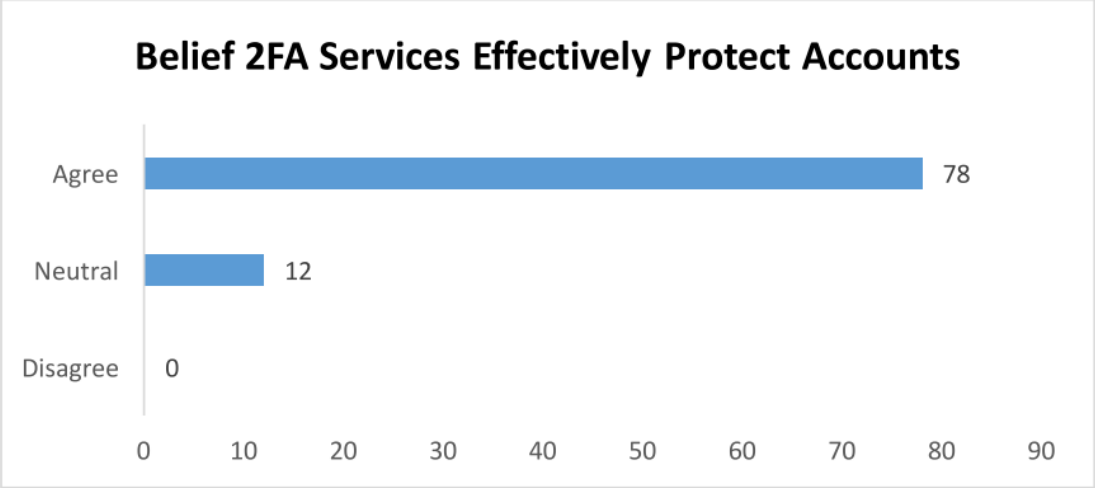
Keeper security, a password manager site, made a list of the most common passwords used and the number one on the list was “123456”. That password was used by almost 17% of users in nearly ten million passwords analyzed). Dropbox also affirmed having less than 1% of users using 2FA in their services (Security, K. 2017).

These percentages show that users are still not familiar with 2FA and might not be aware of the impacts of low security practices. One fact that might be related to this scenario has to do with users perception of security.

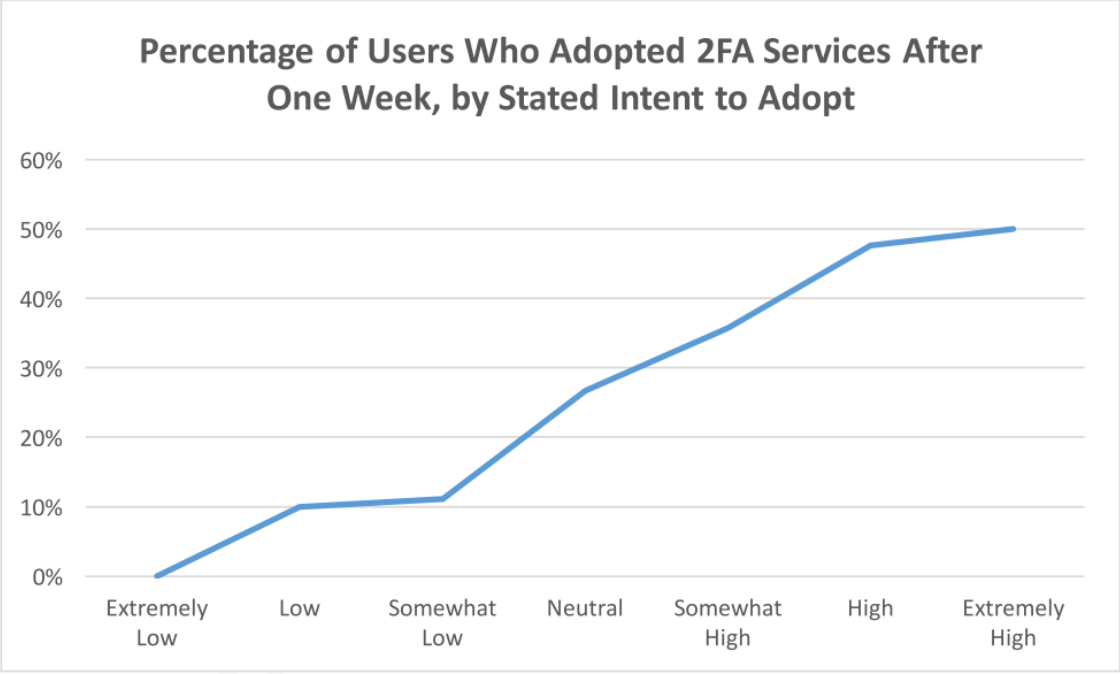
In the paper “Impediments to Adoption of Two-factor Authentication by Home End-Users”, Ackerman (2017) made a research where it was discussed the factors that had influence in user’s decisions to adopt or not 2FA. The research was divided in two phases and had as target audience college students from a university in the United States. The decision to make the research with college students was argued with the fact that students will be the ones entering workforce in a few years so their behavior will have a major impact in organizations.

Their methodology was to show a video to students about 2FA (including advantages, implementation, statistics about cybercrime, among others) and right after that, students would have to respond to a set of questions related to that topic. One of them was if they would adopt 2FA.

The results showed that a message that demonstrates the risks associated with weak security, provides ways to mitigate the problem and demonstrates the ease of implementation of the solution has a positive impact in user’s behavior. Of the 90 participants 87% considered 2FA as an efficient solution and 31% decided to adopt 2FA in the following week after watching the video (Ackerman, 2017).



Graphic 1:Belief 2FA Services Effectively protect Accounts – Source (Ackerman, 2017).



Graphic 4: Percentage of users who adopted 2FA Services after one week – Source (Ackerman, 2017)

2FA provides higher levels of security since attackers cannot have access to users account by just discovering passwords. However, it might make users life more difficult since it will take more time for them to complete their tasks (De Cristofaro, Du, Freudiger, & Norcie, 2013).

2.6.2. Problems of using single-factor authentication

Authentication using just a username and a password (1FA) presents some security gaps. There are many types of attack that aim to gain access to users account and information.

Techopedia, an online dictionary of information technology, describes Brute force attack as a trial-error method where attackers try to guess users password. Attackers can use software to generate a set of combinations, so they can try to crack data that is encrypted but brute force can also be used by analysts to test an organization's information security. Attackers can also try words from a dictionary or try combinations that are commonly used as passwords by users. This method can take some time and uses a lot of computer resources (Techopedia., n.d.).

Melorose, Perroy, & Careas (2015) refer that "Analysis of the passwords used in actual malicious traffic suggests that the common understanding of what constitutes a strong password may not be sufficient to protect systems from compromise". It is important to take remedial measures such as apply password policies and limit the number of attempts users can do to login to their accounts. Although this might reduce this type of attack it might not be sufficient to secure users accounts as there are other forms of attacks.

Another method that can be used for discovering passwords is Key loggers. Key logger is a computer program that records everything that is typed with the intuit of capturing passwords, credit card numbers and other sensitive information. This information is saved in a log file that can be used later for an attacker to use for fraud (Baloch, 2011).

There are also other techniques like Wi-Fi traffic monitoring attacks, cross-site scripting, phishing, among others (Marton & David, 2015). However, we will not enter in more details since it is not the focus of this dissertation. Figure 1 illustrates how 2FA can prevent phishing attacks.

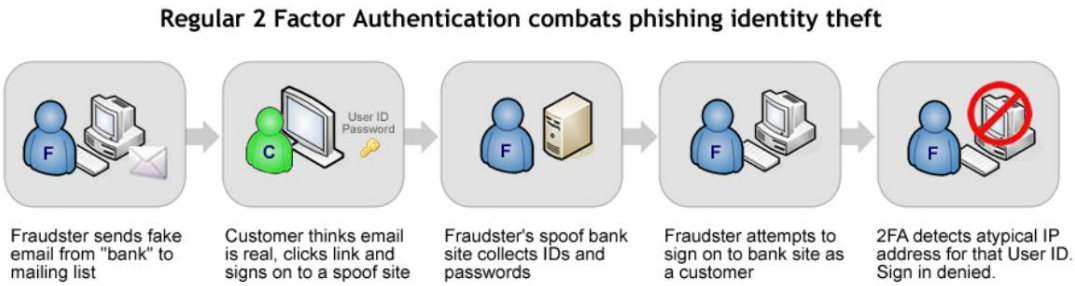


Figure 3: 2FA mechanism against phishing attack example – Source (Authentication, 2006)

2.6.3. 2FA technologies

Several studies have been made comparing 2FA technologies in terms of usability and security.

De Cristofaro, Du, Freudiger, & Norcie (2013) conducted a research on the usability of 2FA. The goal of the authors was to understand the usability of the most popular 2FA solutions, their context of use and motivations. The results of a pre-study interview demonstrated that 2FA's most popular technologies include: codes generated by security tokens, One-Time-Passwords (OTP) that are received via Sms or email and some smartphone applications.

They found that Sms/Email is the most used two-factor among all the others, hardware token is the most common two-factor used at work, Sms/Email is the most common for personal use and that Sms/Email is also the most common for financial use.

When regarding motivation most of the users choose voluntarily to use smartphones applications and Sms/Email but when using hardware tokens most of the users are forced to use it. The authors concluded that two-factor technologies are perceived by users as useful regardless of the motivation or context of use they are used for.

Many services offer the possibility of receiving a OTP by SMS. This is a temporary code that is produced by an algorithm and that changes after a certain period of time. In this case, users cellphone (something that users have) is used as the second-factor since users cannot have access to their account if they don't enter the code received by SMS. SMS verification is still one of the most popular 2FA technologies. It became easy to use since nowadays almost everyone has a cellphone and the process does not take long (Gillin, P.,2017).

However, there might exist some security gaps using SMS as a second-factor since nowadays attackers can create malware to gain access to users SMS and intercept received messages (Hoffman, C.,2017).

Authentication using a code received by Email works in a similar way as authentication using a code received by SMS. The difference is that in this type of authentication users will receive a OTP in their email. They can only access the internet service when they enter the code received.

Hardware tokens can also be used as a second-factor. They are devices that generate a passcode by simply pushing a button. The code changes after a period of time and can be used to access services (Hoffman, C.,2017).

There are also smartphone applications that can be used in order to generate the code to be used in an authentication (e.g. Google authenticator). An advantage of using this technology is that it doesn't need to be connected to the cellphone's network operator (Hoffman, C.,2017).

Every 2FA technology has advantages and disadvantages. However, it is always better to have 2FA implemented than not having this authentication method.
Each organization must choose the 2FA technology that better adapts to their organization (Gillin, P.,2017).

2.6.4. Examples of implementations

The concept of 2FA is not recent, however, its use is gaining more popularity given the digital era we are living in. Many people probably have used 2FA in a variety of activities but never thought of the idea behind this concept.

2FA is implemented in activities such as going to an ATM and making transactions online. If users want to use the ATM for any kind of operation, they'll have to type something that they know (card password) but they also need to have the ATM card (something that they have). In the traditional method, it is not possible to have access to ATM's functionalities without one of those elements (Tsymzhitov et al., 2016).

When making transactions online some banks require users to provide a code (e.g. token sent to cellphone and transactions authentication numbers) in order to complete the operation. This method is also considered 2FA (Dijkstra & Esajas, n.d.).

Gmail also offers now the possibility of using 2FA in accounts. Access to gmail's account is usually done using an email and a password. Now it is possible to apply two-step verification (as it is called by Google) in order to help users protect their accounts. Google has an application called Google Authenticator, a software that uses OTP and implements two-step verification that can be used in the authentication (Gebhart, C. B., 2016).

Some organizations define that there are operations/functionalities that are mandatory to have 2FA on it because it is considered part of the security policies of the business. And because of that users/employees are required to use 2FA in their activities. Those operations/functionalities are usually the ones that involve sensitive and confidential information such as bank transactions and access to email accounts (Attitude, 2005).

2.6.5. Case scenarios

- *E-learning system*

Mayer (2011) and Maqableh et al. (2015) define E-learning (Electronic learning) systems as "the delivery of education in a flexible and easy way through the use of internet to support individual learning or organizational performance goals."

Nowadays, educational institutes have been adopting this system and students are compelled to go along with it since important study materials are available there.
This adoption seems to be having a good impact in student's perspective. Students can manage their time and can access online material everywhere as long as they have internet connection. Some example of Learning systems are: Moodle, Ilias, ATutor, Coursera, Canvas, among others (Marton & David, 2015).
Many question may rise when regarding security in E-learning systems. Do users trust their E-learning systems in terms of security? Do users know if their passwords are transmitted over a secure channel? How can we be sure that an online test or course is being accomplished by the student who is enrolled in it? (Marton & David, 2015).

A research was conducted to study the levels of authentication strength that is perceived by users as the most appropriate to fight impersonation fraud in E-learning systems activities. The E-learning activities that were used were determined in previous studies that identified valuable activities for these systems. The study's findings demonstrated that there are activities in these systems that users consider that have a higher risk of impersonation fraud. Given that, some E-learning activities need higher levels of security strength, that is, more than just a username and password in the authentication process (Beaudin, 2016).

Learning is a continuous process and because of that it is not limited to youth generation. With the expansion of technology, learning is not restricted a time and a specific age group or to a place (Barbosa,2016). We can now learn through online learning systems.

With the expansion of technology E-learning systems are being adopted by more and more educational institutions. Nowadays a variety of institutes give credits to their students after successfully concluding online courses. However, since most of the systems require a username and password in order to authenticate it can become easy for attackers to access users accounts through a variety of ways (Marton & David, 2015).

The above-mentioned authors made a comparison of learning systems in terms of security.

Moodle

Feature	Availability
Password policy	Strong by default
HTTPS support	Yes
HTTPS turned-on by default	No
Brute-force attack mitigation	No
3rd party authentication	Yes, with auxiliary module (OAUTH)
Two-factor authentication	No by core feature set, Yes with auxiliary module via Google account
Other security feature	ReCAPTCHA
2FA / Yubikey integration	Possible via 3rd party authentication method

Table 2: Security considerations of Moodle – Source (Marton & David, 2015).

Ilias

Feature	Availability
Password policy	Not strong
HTTPS support	Yes
HTTPS turned-on by default	No
Brute-force attack mitigation	No
3rd party authentication	Yes
Two-factor authentication	No
2FA / Yubikey integration	Possible via 3rd party authentication method

Table 3: Security considerations of Ilias – Source (Marton & David, 2015).

ATutor

Feature	Availability
Password policy	Strong by default
HTTPS support	Yes
HTTPS turned-on by default	No
Brute-force attack mitigation	No
3rd party authentication	Yes
Two-factor authentication	No
2FA / Yubikey integration	Possible via 3rd party authentication method

Table 4: Security considerations of ATutor – Source (Marton & David, 2015).

Canvas

Feature	Availability
Password policy	Strong by default
HTTPS support	Yes
HTTPS turned-on by default	Yes
Brute-force attack mitigation	No
3rd party authentication	Yes
Two-factor authentication	No
2FA / Yubikey integration	Possible via 3rd party authentication method

Table 5: Security considerations of Canvas – Source (Marton & David, 2015).

Coursera

Feature	Availability
Password policy	Not strong
HTTPS support	Yes
HTTPS turned-on by default	Yes
Brute-force attack mitigation	No
3rd party authentication	No
Two-factor authentication	No
2FA / Yubikey integration	No

Table 6: Security considerations of Coursera – Source (Marton & David, 2015).

Most of the E-Learning system shown in the previous tables have a strong password policy. Although having a strong password policy reduces the risk of password theft by brute force attack there are many other techniques that can be used to gain access to users password.

None of E-learning systems use 2FA directly in their systems. This solution was created in order to mitigate user's problems with long and complex passwords (Marton & David, 2015).

By studying 2FA in E-learning systems we intend to analyze the impact of its adoption in user activities and also understand what functionalities of these systems users consider important to have extra protection. With this case scenario study, we hope to extract import data that can help in the construction of more secure and convenient E-learning systems.

- *Homebanking*

Homebanking is one of the most common context of use of 2FA implementation. However, little research has been made in order to investigate the usability, security and user acceptance of 2FA (Krol, Philippou, De Cristofaro, & Sasse, 2015) .

According to Business Dictionary, homebanking is "The facility to securely access funds, account information, and other banking services through a PC/Telephone over a wide area network or internet" (Business Dictionary, 2017). Homebanking offers a set of advantages to their clients such as: ease access, 24-hours available service and secure transactions. 2FA is currently implemented in a variety of homebanking functionalities. Examples of 2FA implementation can be seen in several homebanking systems, where in order to make online transactions users have to introduce random positions of a matrix. The matrix can only be generated in an ATM.

A research was developed in order to analyze the impacts of 2FA on the adoption of internet banking. In this qualitative study 12 face-to-face interviews were conducted and a set of key factors that could have influence on internet banking adoption were identified and analyzed. The study's findings showed that 2FA did not have a negative effect in the ease of use of internet banking and with the adoption of this mechanism internet banking is still considered convenient by the participants. Moreover, 2FA adoption is not seen as a mechanism that decreases internet banking advantages (Han, Kurnia, & Peng, 2010).

Gunson, Marshall, Morton, & Jack (2011) conducted an investigation about user perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. The results demonstrated that 2FA offers higher security than single-factor authentication. However, in terms of usability single-factor was considered more convenient and easy to use. Although users considered single-factor easy to use, quick and convenient they also valued the extra security that is offered in 2FA.

Krol, Philippou, De Cristofaro, & Sasse (2015) studied the usability of 2FA in 21 UK online banking customers. Users demonstrated some usability issues, in particular with hardware tokens. After conducting a series of interviews, the results obtained demonstrated that there is a negative correlation between user satisfaction and the use of hardware tokens. Users did not like to provide multiple credentials and there was a participant that changed to another bank to avoid using hardware tokens. The authors recommended the reduction of authentication steps

and the removal of functionalities that did not improve security but had unwilling effects in experiences faced by users.

Weir, Douglas, Richardson, & Jack (2010) investigated user preferences for authentication methods but in a more specific scenario, eBanking. Three different authentication processes were compared: two-layer password method (single-factor) and two 2FA solutions. On the one hand results showed that when regarding usability metrics, two 2FA methods have a significantly higher score than single-factor methods for eBanking. On the other hand, the majority of users considered single-factor methods the most convenient option. The results recommended a set of topics to consider when selecting authentication options. They are: convenience, personal ownership and habitual experience of processes.

By studying the implementation of 2FA in homebanking systems we intend to analyze the impact of its adoption in user activities and analyze which functionalities users consider important to apply 2FA.

2.6.6. Mandatory 2FA in online payments

The organizations of European Union (EU) have been demonstrating concerns related to online payment security. This concerns originated two documents: The European Banking Authority Guidelines on the security of internet payments and a revised version of Payment Service Directive (PSD). These documents advocate the mandatory use of a "Strong Costumer Authentication" (SCA) before the process of online payment (Centeno & En, 2016).

European Banking Authority (EBA), "An independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector" (European Banking Authority, n.d.), issued a set of guidelines to make online payment in the EU more secure. These guidelines included the use of 2FA and OTP for online payments in order to ensure a stronger authentication. Low risk transactions (payments that have low values associated) are excluded for the mandatory need for SCA. EU companies had until August 1 of 2015 to search for solutions that included 2FA. EBA had as the basis for the guidelines suggestions from the European Forum on the Security of Retail Payments. One of the causes that motivated this decision was the fact that several statistics showed the increasing

number of data violation. For example, Center Media Data and Society presented a report showing that 570 million entries were stolen only by data theft (Industry News.,2015).

Payment Services Directive, a set of rules defined by the EU for payments, approaches all types of electronic payments (mobile and online payments, card payments, direct transfers, among others). However, unlike EBA guidelines PSD (revised PSD2) does not require mandatory OTP (European Commission., 2017; Industry News.,2015). Table 7 gives a description of the main characteristics of EBA and PSD.

	EBA Guidelines	PSD2
Scope	Payments on the internet	All electronic payments (including face-to-face and remote environments)
Definition of SCA	2 factor authentication, plus a "one time password"	2 factor authentication. For remote electronic payments one of the factors linked to the amount and the payee
Exemptions to the application of SCA	Low-risk transactions: • Under EUR 30 • Risk assessment	Different factors: • the level of risk involved in the provided service; • the amount and/or the recurrence of the transaction; • the payment channel used for the execution of the transaction.
Consequences of Non-compliance	Depends on local Supervisor (e.g. Central Banks)	Local Supervisors; and can be directly invoked by private persons before a National Judge
Liability	Remains silent	The actor in the payments chain that decided not to apply SCA is liable. This is expected to be the Issuer, the Acquirer or the merchant in Visa payments. The consumer is not held liable for unauthorised transactions
Implementation		EBA to draft Regulatory Technical Standards in the 12 months following publication of PSD2. Regulatory Standards to be implemented within the 18 months following their formal adoption
Applicability	August 2015	January 2018

Table 7: European Banking Authority guidelines and Payment Services Directive – Source (Centeno & En, 2016)

2.7. Contributions of the studies

Some of the studies referred in this section have particular interest for the construction of the approach that we propose in this dissertation.

Adams and Sasse (1999) have proposed a set of recommendations regarding password policies. The aim of these recommendations is the construction of secure passwords. These authors argue that the construction of secure passwords can be achieved by providing instructions and training

on constructing secure and memorable passwords. It is important to provide constructive feedback during online password construction and give users explanation if a password is rejected. The authors also recommend ways of ensuring that users implement security mechanisms. However, it is necessary to understand their perception of security. Actions like informing users about potential threats to the systems and explaining which systems and assets are sensitive can increase user awareness of the importance of security.

Since we are developing an approach where we give users the opportunity to choose which functionalities should have 2FA on it is necessary to help them acquire basic knowledge of security (such as the concept, importance and some statistics related to cybercrime) and 2FA (such as the concept, importance and implementation). And by doing that we are trying to understand and increase their perception of security. Our goal is aligned with one of Adams and Sasse's recommendation since we want to increase the adoption of a security policy (2FA).

The security assessment model, "House of security", proposed by (Ang et al., 2007) provided results that validate the need for increasing and making unanimous users perception of security, which is one of the objectives we propose.

Webra tool, the web-based risk analyses tool for home users, developed by Magaya, R. T., & Clarke, N. L. (2012), has some characteristics that are similar to the goals we want to achieve. This tool aims to provide recommendations in order to improve security practices. When Webra tool provides the outputs/recommendations of the risk rating for the assets it is also demonstrating the advantages and disadvantages of protecting these assets. Besides this, it demonstrates which assets are not safe and provides missing controls for them. Our output will be the discussion of the impacts (advantages, disadvantages and consequences) of 2FA in order to try to discover/present ways to ensure more secure and convenient E-learning and homebanking systems.

The study developed by Ackerman (2017) to discuss the factors that influenced the adoption or not of 2FA provided some important inputs that helped the development of the experimentation that is going to be conducted in order to test the approach with users. Their methodology motivated our experience since the author demonstrated the importance of discussing with users about 2FA and according to him "A message which clearly identifies risks on personal level, provides mitigating measure, and demonstrates the ease of implementation, did result in a change in behavior for a significant number of users".

Marton & David (2015) research on security considerations and 2FA opportunities in E-learning environment highlighted that this system can contain personal information and that the number of identity theft has been increasing. Their approach on opportunities for 2FA in E-learning systems motivated our analysis on the implementation of 2FA in E-learning systems and on users choice of the functionalities that they would rather have this mechanism in this specific system.

When regarding homebanking systems Krol, Philippou, De Cristofaro, & Sasse (2015) argued that little research has been made in this field to study the security and usability of this system. With our analysis of 2FA implementation in homebanking systems we expect to add important findings to this field of study.

Employees/Users are often the weakest link when it comes to the protection of information (Metalidou et al., 2014). Because of that, it is important to discuss if we aren't compromising information security by giving users the possibility of choosing system's functionalities that should have 2FA on it.

Users often compromise security of information systems without even knowing that. This happens because security policies implemented might be very rigid and/or because users are not taught how to use the systems. Besides that, users do not have enough information about security problems and what they know might be security threats (Adams & Sasse, 1999).

Many organizations think that employees need to know as little as possible about the security details of the company. However, it is that company's attitude that makes users security behavior less appropriate. In order to change this, it is necessary to communicate more with users and address the importance of an appropriate security behavior (Adams & Sasse, 1999).

We intend to bring some components of the studies that were made by the above-mentioned author to this research. In order to improve users security behavior, we included in the experimentation a presentation of 2FA and other related concepts. This presentation will be made in order to explain these concepts to users and discuss with them the variety of aspects involved.

The following table presents some of the studies discussed in this chapter, their objectives, conclusions and contributions to this study.

Citations	Objective	Conclusions	Contributions
Adams and Sasse (1999)	Study what makes users compromise computer security systems as well as remedial measures to be adopted.	Users do not create strong and secure passwords because they are not conscious of the problems that can be caused by lack of password security.	The recommendations provided are guidelines to the implementation of successful password policies.
Ang et al (2007)	Identify similarities and differences regarding the perceptions of security by different members of an organization.	Different people in an organization have different perceptions and awareness regarding their own company's security.	Results validate the need for a framework for discussing the impacts of security policies in user activities.
Maynard & Ruighaver (1999)	Study the process of security policies assessment.	The criteria used for evaluating security policies may vary depending on the context of the organization.	Evaluation will determine if the approach presented is successful.
Magaya, R. T., & Clarke, N. L. (2012)	Develop a web-based risk analysis tool for home users in order to improve user's security posture by analyzing key assets and provide an overall risk rating for these assets.	Most of the users found the tool useful to assist them with protecting their cyber assets. Users also found the tool easy to use and could be used with minimum security knowledge.	Demonstrates the advantages of protecting cyber assets. Example of a tool to assist a specific community (home users) with protecting their cyber assets.

Petsas et al. (2015)	Quantify the adoption of 2FA on Google.	2FA has only been adopted by 6,4% of users.	Results demonstrate the need for increasing 2FA adoption.
Ackerman (2017)	Study the factors that has influence in user's decision to adopt or not 2FA.	Of the 90 participants 87% considered 2FA an efficient solution and decided to adopt 2FA.	Provided a methodology to analyze the factors that influenced users to adopt or not 2FA.
De Cristofaro, Du, Freudiger, & Norcie (2013)	Study the usability of the most popular 2FA solutions, their context of use and motivation.	Two factor technologies are perceived by users as useful regardless of the motivation the context of use.	Provided findings on the most popular 2FA solutions.
Martin & David (2015)	Propose 2FA implementation in E-learning systems.	Data protection can be done with little steps by using 2FA. It is important to raise users awareness on security.	Findings on 2FA opportunities in E-learning systems.
Han, Kurnia, & Peng (2010)	Analyze the impacts of 2FA on the adoption of internet banking.	2FA does not have a negative effect in the ease of use of internet banking. Even with 2FA implemented, internet banking is considered convenient.	Findings on 2FA implementation and impact in internet banking.

3. Proposed approach

3.1. Introduction

This chapter describes an approach to discuss the impacts of IT security policies in user activities.

The chapter starts by describing the general framework to analyze security policies in terms of usability and security in order to understand the impacts of its adoption in user activities and to recommend the most convenient one to the organizational context.

The third section describes the application of the general framework to two-factor authentication (2FA) security policy.

3.2. General framework

We propose a framework for analyzing IT security policies in terms of usability, and security enabling the discussion of the impacts of security policies in user activities. This analysis is then used to help deciding which policy to adopt and/or justify the choice made. Another object of this framework is to improve security awareness in the human resources of an organization.

This framework can be used by organizations that will implement information security policies for the first time or organizations that had previous experiences with security policies and want to know if the right security policy is being used considering their scenario. This framework is also applicable to organizations that have decided to change to another security policy and are searching for advices. This framework considers the following aspects as inputs: type of data involved (public or private data), expected user behavior versus real user behavior, experiences faced by users versus real user behavior, the information security policy being used/information security policy that the organization wants to use. It is important to try to anticipate possible difficulties users will face when using a specific IT security policy.

This framework will have three activities associated. The first activity consists in requesting user inputs. These inputs will be given to the system in the form of questionnaires. Users will have to respond to a series of questions about their past experiences with security policies, their

expectations about future security policies and their experiences with the current security policy. These inputs will vary depending whether users want to decide the best security policy to use or want to know if they are using the right one for their scenario. A set of appropriate security policies for the organization's scenario will also have to be given to the system. This input will be very important since the tool will have to recommend the most appropriate security policy based on what is the right policy in terms of security and in terms of human aspects.

The second activity consists in analyzing the inputs. This analysis will be done using machine learning tools.

The third activity consists in generating the outputs/recommendations to users. Depending on the cases, the outputs will recommend the most appropriate security policy to use or make a brief statement about the security policy being used.

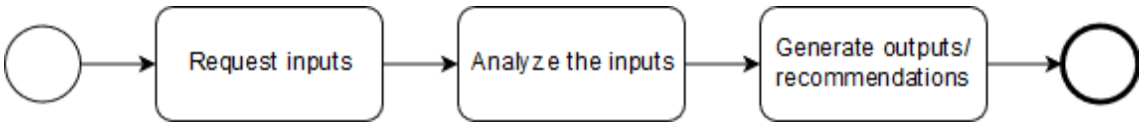


Figure 15: Global view of the process using BPMN

This process may be iterative since the output will be confronted with users expectations. If the outputs/recommendations correspond to users expectations the process will end, if it does not correspond, another analysis will be made in order to obtain other outputs/recommendations.

The first validation concerning users expectations will be made after the system presents the output/recommendation for the first time. Users may have forgot to introduce some inputs that lead to an output that didn't correspond to their expectation. In this scenario, users will have the chance to go back and introduce the missing inputs. After this, another analysis will be made, and another output will be presented.

If the output satisfies users expectations the security policy recommended will be implemented and adopted by the organization. Organizations will determine the time necessary for the recommend security policy to be implemented and adopted by every employee in the organization. After that period of time, organizations will determine if the security policy satisfies users expectations and how successful it has been. If the validation is positive the

process finishes, if it isn't, users expectations are analyzed again and other outputs/recommendations are produced.

Figure 4 extends the request inputs activity and demonstrates the inputs given when the final output is the most appropriate security policy to use according to the organization's scenario.

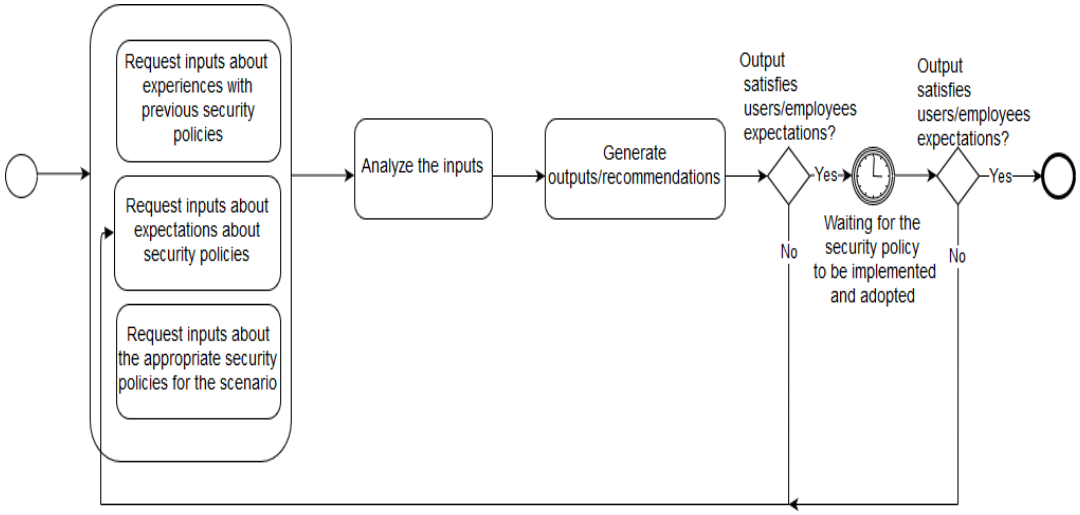


Figure 16: Global view of the process using BPMN

A key concern when proposing such a framework: How can we argue that the framework produces good tools? According to Magaya & Clarke (2012), "A key characteristic of a tool is usability." This means that the interface needs to be easy to use, understand and operate. Jakob Nielsen defines usability as "A quality attribute that assesses how easy user interfaces are to use." (Nielsen, 2012). The interface of the tool also needs to be simple, intuitive and reliable. It is important that users with no prior understanding of security, use the tool with as minimum problem as possible. The recommendations provided should represent appropriate security policies.

This means that these security policies should be the most adequate to the organizational context and prioritized according to risk evaluation. This risk evaluation has to include the human context of the organization (users perception of the policies, impact on users activities, users security awareness, etc.). Another objective of this framework is to improve security awareness in the human resources of an organization.

We consider the framework to be successful if it produces tools that have good usability, provide appropriate security policy advices and improves user security awareness.

3.3. The general framework applied to 2FA

The general framework seeks/recommends the best security policy to be applied in an organization, considering the impact of the security policy in users activity.

Security policies define a set of security methods to be used to protect data. In this section, we describe how we used the general framework with a security policy, 2FA, in two different contexts: E-learning and homebanking systems.

We applied the general framework to 2FA, in particular for the collection and analysis of the impacts of the implementation of 2FA in user activities. We aimed to collect and analyze the impacts of 2FA in terms of usability and security. In this implementation we give users the possibility to choose which functionalities of a system should have 2FA implemented.

The experimentation conducted for the application of the framework to 2FA aims to give internet services users the possibility to choose between 1FA vs 2FA, enabling users to choose the balance between (more) security vs (less) usability.

This experimentation was conducted considering that there are functionalities that the organization who provides the service can only grant access if 2FA is used. In these functionalities users can choose between having access to the functionality using 2FA or not having access to it. An example of this situation is the functionality that enables making transactions in homebanking.

We hypothesize that this approach will increase the adoption of 2FA because users can apply it only on data that they consider important.

An important aspect to emphasize about this approach is that although users have the possibility of choosing the functionalities that should have 2FA on it, this choice cannot be made for the functionalities where 2FA is mandatory.

This happens because there are functionalities from certain systems where the implementation of 2FA is mandatory. There were defined standards in order to stablish which functionalities should have this security policy.

This means that, users will have two possibilities:

1. Choose 1FA or 2FA for the functionalities that don’t contain mandatory 2FA;

2. Choose between having 2FA or not having internet access to functionalities where 2FA is mandatory.

On the one hand, the first possibility reflects a scenario where 1FA is implemented by default. In this case, users can choose between keeping 1FA or implementing an extra step to access the functionalities (2FA). This choice can be made according to users perception of security and/or according to the importance that the functionalities have for them. By giving users this possibility we intend to analyze which type of functionalities users prefer to implement 1FA and 2FA.

On the other hand, the second possibility reflects a scenario where some organizations make 2FA mandatory for an internet service or for given functionalities of it. This happens because they consider important to add an extra layer of security given the relevance of the data. In this scenario, we want to analyze if users will still want to access the information or if they would rather not have access to that functionality given the fact that has 2FA implemented.

4. Evaluation

4.1. Introduction

The previous chapters described the research that is going to be conducted and the related work in this field. Moreover, the general framework was explained and the proposed approach for this research was described.

This chapter presents the evaluation conducted to analyze the two-factor authentication (2FA) mechanism as an IT security mechanism in terms of usability and security in user activities.

The evaluation was done through experimentations with users. An overview of the activities of the experimentation and a brief description of them is presented. The chapter also presents a description of the experimentation in action including the face-to- face and long-distance experimentations that were conducted.

This chapter concludes with the presentation of the results obtained in the quantitative and qualitative study.

4.2. Goals

The goal of the evaluation was to make an attempted to understand the problems behind our research questions in order to analyze the impacts of 2FA in user activities in terms of usability and security. Besides that, we wanted to test the possibility of users deciding which systems functionalities should have 2FA on it.

We present below the research questions of this research.

1. How does 2FA affect user activities in terms of usability and security?

With this research question, we wanted to understand what are users perceptions of 2FA advantages and disadvantages in their activities. We also wanted to analyze the ease of use of 2FA and users security perception of this mechanism. That is, if they felt any constraints while using this mechanism and if it is perceived or not as an advantage in terms of security.

2. Is it a good approach to provide users with the possibility of deciding between:
    a. 1FA or 2FA for a certain functionality of a system;
    b. 2FA or not having internet access to the functionality of the system,

    in order to minimize the negative impacts of its adoption in user activities and to increase user experience and user acceptance regarding security aspects?

With this research question, we wanted to make an attempt to understand the users preferences in terms of system functionalities to which they would want to apply 1FA or 2FA. Besides that, we also wanted to understand what would be the users choice when confronted with the possibility of using a functionality that has mandatory 2FA or not having internet access to that functionality.

3. What is the knowledge that the users have about the 2FA and 1FA concepts?

With this research question, we wanted to understand the users level of knowledge of the 2FA and 1FA concepts and if the users have had contact with these concepts before the experimentation. We wanted to understand if this experimentation could improve their knowledge on these topics.

4.3. Research methodology

We chose as research methods: descriptive research and a mix of qualitative and quantitative research (Nallaperumal & Krishnan, 2013).

Descriptive research is used to give a description of the current state of affairs. It can be seen as an attempt to identify or determine the reason of some problem or phenomenon. This type of research can be done using surveys in order to reach fact-findings (Nallaperumal & Krishnan, 2013).

We want to discuss the impact of 2FA in user experience and because of that it is necessary an approach where we can understand user preferences and knowledge in this area. One of the methods of descriptive research is the survey. We implemented a survey to investigate about these preferences and knowledge.

In quantitative research, the interest is on discovering facts that can be expressed as numerical data. A qualitative research has interest on understanding human behavior and has a subjective

approach since it makes a description of the problem or phenomenon from the perspective of those who are experiencing the problem or phenomenon (Nallaperumal & Krishnan, 2013).

We used a mix of quantitative and qualitative research.

In this research, we used the exploratory nature of qualitative research since our objective was to understand a problem (impact of 2FA in user activities) and examine our research question in different levels of depth. Thematic analysis was used and the six steps for conducting thematic analysis from Braun & Clarke (2006) were applied.

One the one hand, when trying to understand questions like: the impact of 2FA in user experiences, user awareness of 2FA and internet security, and the functionalities users would choose to have 2FA on it, we made an attempt to understand users behavior and the reasons that led to a certain way of thinking. By doing we used qualitative approach.

On the other hand, we expected to find numerical results like: percentage of users that are familiarized with the concept of 2FA, percentage of users using 2FA, percentage of users that consider the impact of 2FA in their experience positive (or negative), among others. By trying to get these results we conducted a quantitative research.

According to Hevner, March, Park, & Ram (2004) "The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well executed evaluation methods.". These authors propose a set of evaluation methods and in this dissertation, it was used: informed argument and scenarios.

In an informed argument method, it is necessary to use important research in the area in order to develop a strong argument for the utility of the artifact. The literature review chapter gives an overview of some studies made on user experience about security policies and in particular 2FA. A lot of those studies refer to the disadvantages of not giving importance to the human factor when building and using security policies. We consider that the studies investigated for this dissertation contain the necessary information to argue the utility of this dissertation's approach.

In scenarios method, in order to evaluate the artifact there is a need to "Construct detailed scenarios around the artifact to demonstrate its utility" (Hevner, March, Park, & Ram, 2004). In this dissertation, we proposed the analyses of two case scenarios (a university student web portal and a homebanking system) to argue the utility of the approach that we propose.

Since in the research question we asked, “What would be a good approach to provide users with the possibility of deciding between two options?", it is necessary to define what is a “good” approach in this case.

We considered the approach good if it has a good usability, is perceived by the majority of the users as being useful and increases users knowledge on security.

4.4. Experimentation description

With this experimentation, we wanted to understand/analyze the impacts of 2FA in user experiences/activities in terms of usability and security. To understand its impacts, we developed an approach where we gave users the possibility of choosing certain functionalities of systems to apply 2FA on it. We formulated some research questions (described in sub-section 4.2 Goals) and tested them by analyzing two case scenarios: a university student web portal and a homebanking system.

By giving users the possibility of choosing functionalities that they would rather have 2FA on it we intended to analyze:

1. Users perception of the 2FA mechanism and how it affects user activities in terms of usability and security.

2. Impact of this approach: We hypothesize that this approach will increase the adoption of 2FA, because users can apply it only on data that they consider important.

The experimentation had a series of activities, however, these can be summarized in three big blocks:

- Discussion/Analysis of 2FA as an IT security policy.
- Demonstration of 2FA implementation and description of the case scenarios.
- Analysis/Description of 2FA security and usability.

Two case scenarios were considered for the experimentation: a university student web portal, having as target audience college students and a home banking system, having also as target audience college students that use this system.

The activities of this experimentation were:

1. Introduce the research that is going to be conducted.
2. Show presentation about 2FA.
3. Present Java program.
4. Ask users to respond to introductory questionnaire.
5. Ask users to respond to E-leaning and/or homebanking questionnaire.

After introducing the research, a presentation about 2FA was made. In this presentation, it was explained what is 2FA, its importance, how it works, some examples of enterprises that currently use this mechanism and the case scenarios that were analyzed in this dissertation.

With this presentation, we intended to introduce this concept to users that are not familiar with it and/or clarify all the doubts that may exist about the covered concepts.

Following the above mentioned activities, in activity 3 the participants were presented with an application that demonstrates how 1FA and 2FA work, including the extra steps that 2FA requires. This application was developed in Java using javax.mail and javax.mail.internet packages.

After that, the participants responded to an introductory questionnaire where they demonstrated their knowledge and experience on this topic.
Following this activity, the participants had to respond to two other questionnaires: one about E-learning systems and the other about homebanking systems.

In each of the questionnaires participants were presented with a set of interfaces, each of them containing functionalities related to the testing scenario and they had the possibility to choose which functionalities they think should have 2FA implemented.

By doing the first three activities of the plan we expected to meet the following objectives proposed: Increase user awareness of internet security, increase user experience with the services provided by the internet, including its security, and analyze user awareness of security advantages of 1FA and 2FA, as well as its impact in user activities.

The last two activities were done in order to analyze user awareness of security and usability of 1FA and 2FA, its impact, and analyze the implementation of 2FA in a university student web portal and in an homebanking system.

Each activity can be included in the three big blocks that give an overall view of the experimentation phases.

Discussion/Analysis of 2FA as an IT security policy: Since this is a topic that might not be understood by the overall target audience it is necessary to explain and discuss with participants this concept before giving them the opportunity to answer to the questionnaires. We wanted them to understand the topic and the basic related concepts such as information security in order to try to understand their real opinion in the questionnaires.
The activities that were included in this block are activity 1 and 2.

Demonstration of 2FA implementation and description of the case scenarios: After discussing with participants about 2FA, we considered that it is important to give them the possibility to see its implementation in a practical context. "Practical knowledge can often lead to a deeper understanding of a concept through the act of doing and personal experience" (Bradley, 2012). Given this, users might have assimilated better this concept since they had both a theoretic and practical approach.
The activities that were included in this block are activity 3 and 5.

Analysis/Description of 2FA security and usability: The basis of our discussion of results was the outcomes received from the questionnaires. Based on these results, we made an analysis on 2FA security and usability. We developed three questionnaires: an introductory questionnaire, an E-learning system questionnaire and an homebanking questionnaire. The activities that were included in this block are activity 4 and 6.

4.4.1. Target audience

The target audience chosen for this experimentation were college students. In the E-learning system scenario the target audience was college students since they form one of the communities the system was built for.

College students can also have homebanking systems. Given this, they can also be considered the target audience in the homebanking case scenario.

4.4.2. Questionnaires

The method used for data collection was experimentation with users. This experimentation included questionnaires that were responded by users.
We developed three questionnaires for this experimentation. Each one to be used in a different moment of it.

A pilot experience was conducted with three users in order to analyze possible gaps in the experimentation and improve the questionnaires quality. By making a pilot experience we also wanted to see if the questionnaires were understandable and coherent. Users that participated in this pilot experience had the same profile as the ones who participated in the final experimentation. However, users from the pilot experience were not part of the final sample of users.

Users opinion on the pilot experience originated the final versions of the questionnaires. The questionnaires were developed in Google Forms and were answered online.

The first questionnaire was an introductory questionnaire (Appendix A: topic 3) where users demonstrated their knowledge on 2FA. The objective of this questionnaire was to understand if uses have had contact with this mechanism before and what was their experience with it. For users that have never had any experience with 2FA we wanted to understand if, after a presentation on this topic, they considered this mechanism important and if they considered useful the security increment that this mechanism introduces. With this introductory questionnaire, we also wanted to understand users awareness on information security.

The second and third questionnaire (Appendix A: topic 4 and 5) were about the case scenarios that were analyzed: E-learning and homebanking systems.
For these questionnaires, we developed interfaces that have similar functionalities as the real systems. The functionalities for the E-learning system interface were: *Personal Area, Courses* and *Grades*. For the homebanking system interface the functionalities are: *Check balance and transactions*, *Transactions* and *Payments*. We also developed sub-functionalities for some of the main functionalities.

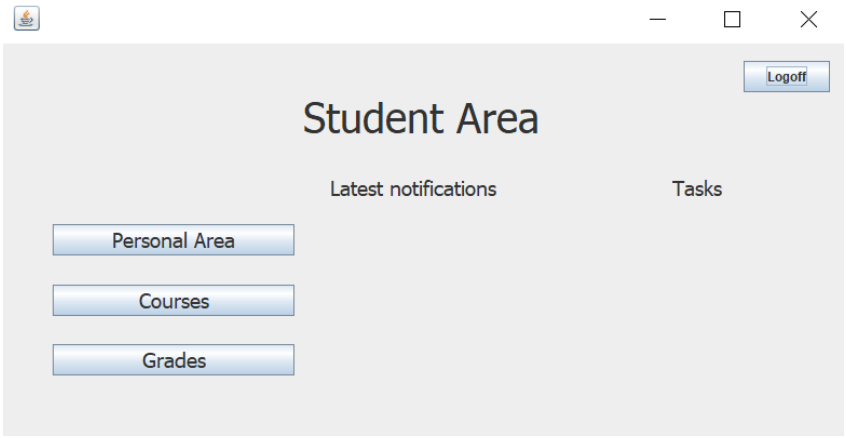


Figure 6: Main interface for E-learning system

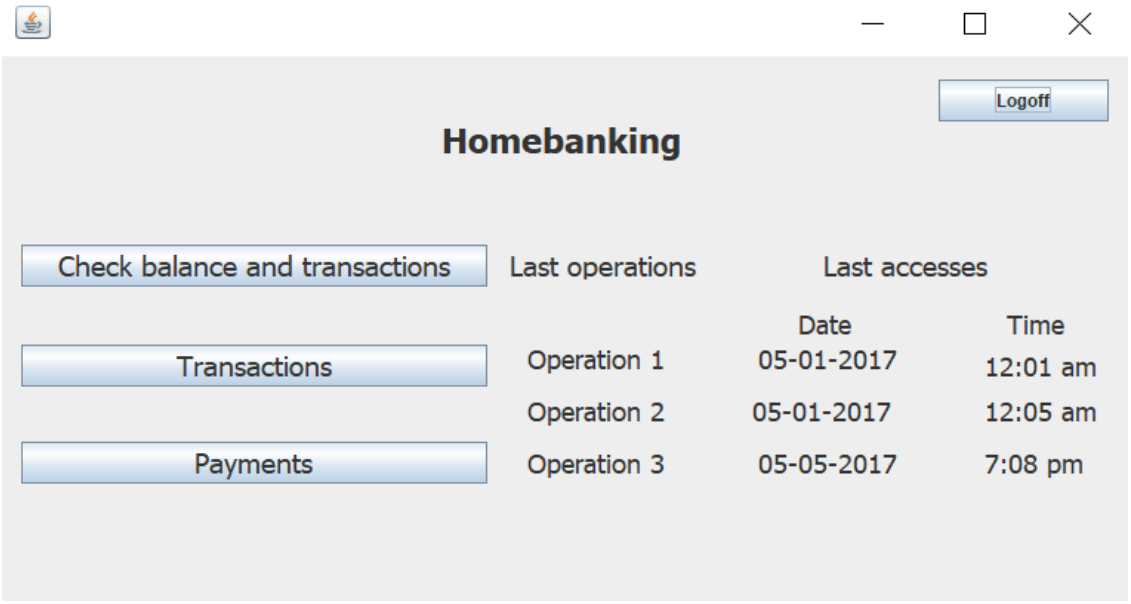


Figure 7: Main interface for Homebanking system

By creating these interfaces, we wanted to construct realistic scenarios for users so they would have better experiences (since by having an interface they can relate it with their real E-learning/homebanking system) while choosing which functionalities should have 2FA on it.

In addition to having interfaces where users could choose which functionalities should have 2FA on it, these questionnaires had also questions to try to understand the experiences users go through when using a functionality that has 2FA on it. These questions were characterized by a five-level Likert scale answer (one to five – Very poor to Excellent). The questionnaires also

presented open questions where users could express their opinion on this topic. These questions were not mandatory to answer.

The interfaces for the questionnaires were developed using Windows Builder.

4.4.3. 2FA and 1FA demonstration using a Java application

A Java application was created in order to stablish an analogy with scenarios where 2FA is implemented. This application was created to demonstrate users how 2FA works. This program supposes users had a successful login, and because of that, the first interface shown after running the program corresponds to the first interface shown after login. The second reason to create the demonstration as an application was: an application was easy to distribute through a computer or cellphone.
The interfaces were created using Windows Builder and the program was developed using Java.

The figure below presents a system with two available functionalities. *Functionality 1* had 1FA associated and *Functionality 2* had 2FA associated.

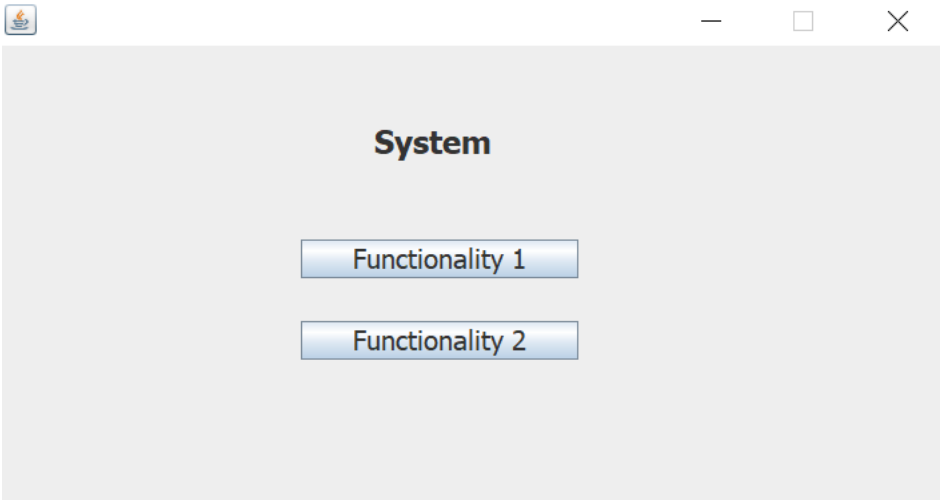


Figure 8: Prototype of a system with two functionalities

When users clicked *Functionality 1* button would have direct access to *Functionality 1* screen. In this case, it was applied 1FA since users only had to authenticate one time (login process).

Figure 9: ''Functionality 1'' screen

This means that in real systems users would have direct access to the features that *Functionality 1* offers.

When *Functionality 2* button is clicked users would be redirected to a screen where they would have to provide their email and click the button *Continue*.

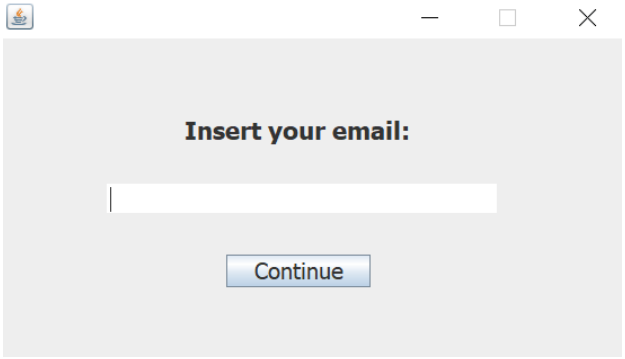


Figure 10: "Insert your email'' screen

If no email was provided, the program would present a message informing users that they had to introduce their email in order to proceed to the next screen, as it is shown in figure 11.

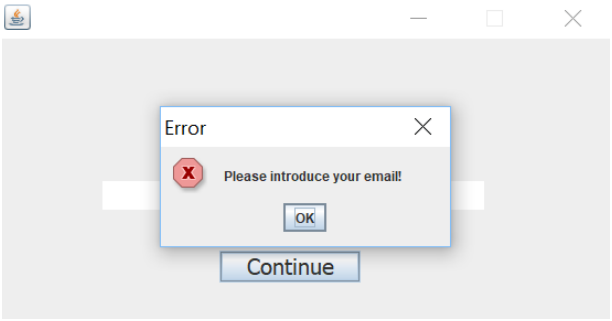


Figure 11: Introduce email error

After introducing the email, users would receive a verification code in the email that was given in the previous interface. They would have to type the code received in the text area and click button *Continue.*

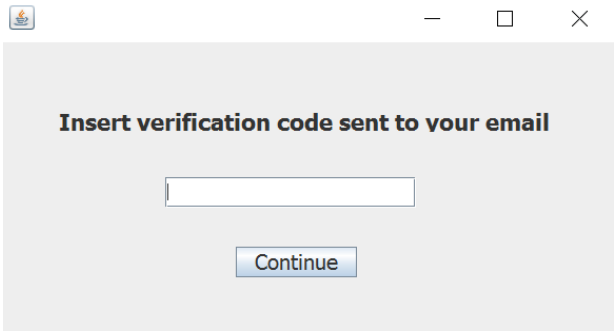


Figure 12: "Insert verification code" screen

If the verification code did not correspond to the one sent to the email or if users pressed button *Continue* without entering the code an error message would be presented, as figure 12 shows.

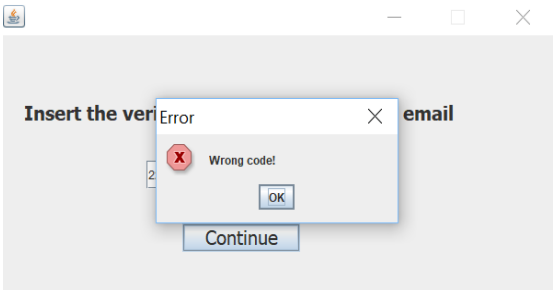


Figure 13: Wrong email error

If the verification code provided corresponded to the code sent to the users email, they would have access to Functionality 2 and could navigate freely on that functionality. Functionality 2 window is shown in figure 14.

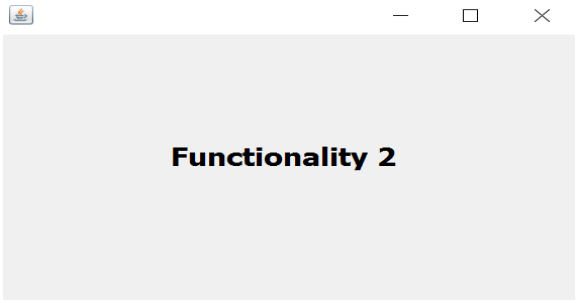


Figure 14: "Functionality 2" screen

4.5. Experimentation in action

This experimentation was conducted from the beginning of July 2017 until the end of August 2017. We received a total of 27 valid answers to the questionnaires and we also received feedback from users during and before the experimentation.

We conducted two different types of experimentations: long-distance and face-to-face experimentations.

In an early stage of this research we planned to conduct only face-to-face experimentations. However, since we conducted the experimentations during holiday breaks we added long-distance experimentations, so we could contact more people.

4.5.1. Face-to-face experimentations

The participants for this experience were recruited by the investigators through talking to groups of students from different universities in Lisbon, former students of ISCTE-IUL and other colleagues.

People were invited to participate in an experimentation that took place at ISCTE-IUL.

We conducted 3 sets of experimentations and each experimentation took about thirty-five (35) minutes. In each experimentation, there were three (3) to five (5) participants. Each participant had a desktop computer from ISCTE-IUL computer laboratories to use during the experimentation (to use the Java program and respond to the questionnaires). We considered better to conduct sets of experimentations (with few people) instead of conducting a single one.

In the beginning of the experimentation, it was explained the objectives of this research and what it consisted of. After that, the participants had the opportunity to ask and clarify any doubt about the research or/and the procedures of the experimentation.

The experimentation proceeded with a presentation about 2FA, with the contents described in sub-section 4.4.

The objective of the presentation was to help the participants understand some basic concepts of 2FA in order to help them respond to the questionnaires.

The presentation was followed by a demonstration of how 2FA works using a Java program. After the demonstration, the participants had the opportunity to test the program.

After they tried the Java program, participants had the opportunity to clarify the doubts that might still existed about the covered aspects, and make comments in order to move to the next step of the experimentation: respond to an introductory questionnaire.

In the last part of the experimentation the participants had to respond to the questionnaires of the case scenarios. Students that did not use homebanking systems could just respond to the E-learning system questionnaire. Students that used both systems would have to answer to the E-learning and homebanking system questionnaire.

4.5.2. Long-distance experimentations

The participants for long-distance experimentations were contact by Facebook and by sending emails to ISCTE-IUL students. We asked the participants to forward the invitation of the experimentation to other people that were part of the target audience, so we could reach a considerable number of participants.

It was created a shared folder in Dropbox that contained three documents: research protocol (Appendix A: topic 1), a power point presentation about 2FA (Appendix A: topic 2) and instructions on how to proceed to complete the questionnaires (Appendix A: Topic 6).

The research protocol document contained a description of this research, its objectives and a description of how the experimentation will be conducted.

The power point presentation about 2FA had the objective of introducing this topic to users (in case users have never had contact with this topic) and help them understand the basic related concepts. This presentation was very important to help users answer to the questionnaires.

The instructions document contained the steps that the participants needed to take in order to complete this experimentation.
It started by asking users to read the research protocol document. This way, users could know what to expect during the experimentation. It then asked users to read the power point presentation and watch a video demonstrating 2FA applied to functionalities of a system.

This video contained the demonstration of how 2FA works using a Java program, that users had the opportunity to test in face-to-face experimentations. Since users had to have Java installed in their computers to use the program (and not everyone has it in their computers) we recorded a video where we gave the same steps users would had to take to understand how 2FA works. The video was uploaded to Youtube and a link to the video was provided in the instructions document.

After that, the instructions document asked users to answer to the introductory questionnaire.
If users used E-learning and homebanking systems they would have to answer both questionnaires. Otherwise, they would just had to answer to the homebanking questionnaires.
The instructions document provided the Google form's links to the three questionnaires.

The link to the Dropbox folder was given to the participants at the beginning of the session and we asked them to follow the instructions contained in the instructions document. The participants could ask any questions or make commentaries during the experimentation through Facebook or email.

At the end of it, if the participants had any feedback or commentaries they could send a message by Facebook/email.

4.6. Data analysis

In order to analyze our data, it was applied mixed method (mix of quantitative and qualitative method). The answers from the questionnaires and the feedback and comments made during the experimentation were our main source of data. The quantitative study was made using SPSS 20 and the qualitative study was conducted using Thematic analysis.

4.6.1. Quantitative analysis

The results of the closed questions of the questionnaires were transferred to SPSS 20 where we proceeded to the statistical analysis.

4.6.2. Qualitative analysis

Braun & Clarke (2006) describe thematic analysis as "A method for identifying, analyzing, and reporting patterns (themes) within data."

The above-mentioned authors published a paper where they approached how to conduct thematic analysis for researchers that are new in this area. They provided a step-by-step guide for doing thematic analysis. To analyze our data, we followed this guide (six steps).

In the earliest phases of this analysis, it was created a document where all the open answers to the questionnaires and comments made were placed. After that, data was read and re-read many times in order to get familiarized with it. It was also taken some initial notes of possible patterns on the data to help going to the next stages with some basic ideas of what could be possible themes. This stage corresponds to the first step of the guide.

The step after the stage of familiarizing with data, is finding codes in data (step 2). Codes are features of the data that might be interesting to the researcher/analyst. They are normally words, short phrases and metaphors that allow the organization of data in relevant groups (Braun & Clarke, 2006).

We created a table where in a column it was listed all data items (single answers from the data set) and in another column, it was listed the codes identified (Appendix B: topic 1). Each line of that table contained a data item and initial codes identified. It was used highlighters to identify possible patterns and data extracts (segments of data) that were coded.

After the coding phase, codes were organized in order to, when combined, form a theme (step 3). A theme describes relevant aspects of the data, and that is related to the research question. In this stage, it was constructed a thematic map to help visualize the relationship between codes and themes and help organize/group possible themes (Braun & Clarke, 2006). Figure 15 shows an example of a thematic map (in fact, the final version of it). Some codes that were identified in the coding stage were transformed into themes.

In the next stage (step 4), we tried to allocate codes into themes. However, there were some codes that seemed not to fit in any themes. For those codes, it was created a theme called 'miscellaneous' to place them since it could be found a theme for them on next stages. Some sub-themes also emerged.

After creating an initial list of themes, that at this point didn't have concrete names (just a word to remind us what we were looking for) since this wasn't the final iteration of the thematic map, it was necessary to review the candidates for themes.

When reviewing the thematic map, some themes disappeared because there weren't sufficient data to support it and others emerged. It was also reviewed all of the data extracts that were coded. It is important to analyze if with the themes, subthemes and codes, it is possible to tell a story about the data and relate it with the proposed research question (Braun & Clarke, 2006).

In step 5 it was time to define and name the themes. The thematic map was reviewed and the last version of it appeared (Figure 15). The themes were defined and it was given names to them to express the story about the data that each one of them was going to tell.
In order to see if the themes were coherent and concise it was made an attempted to describe them in small phrases.

The last step (step 6), was the production of the report. In this stage, it was used data extracts to give examples and to help describe the identified themes. This step will be presented in the Results sub section.

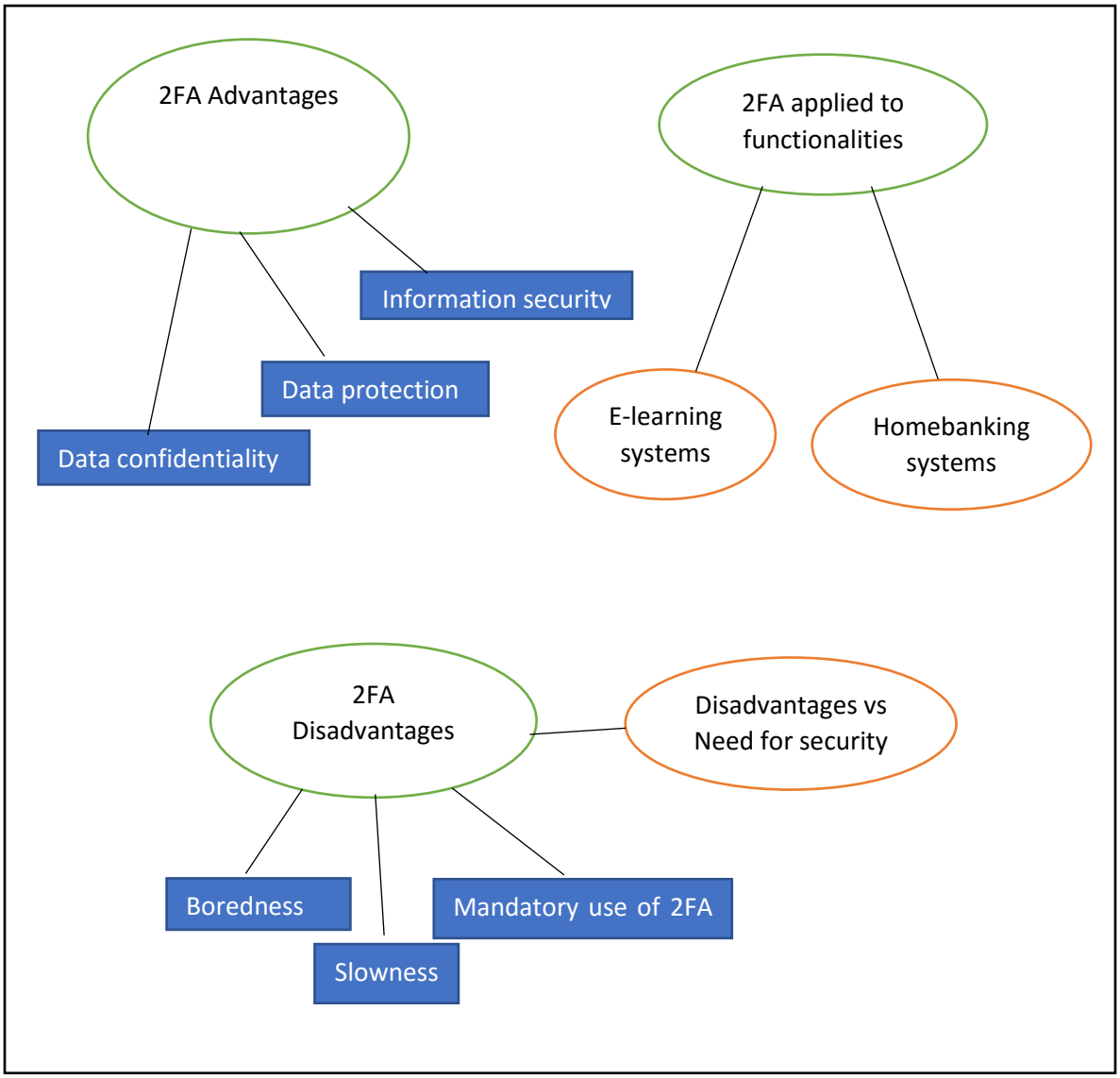


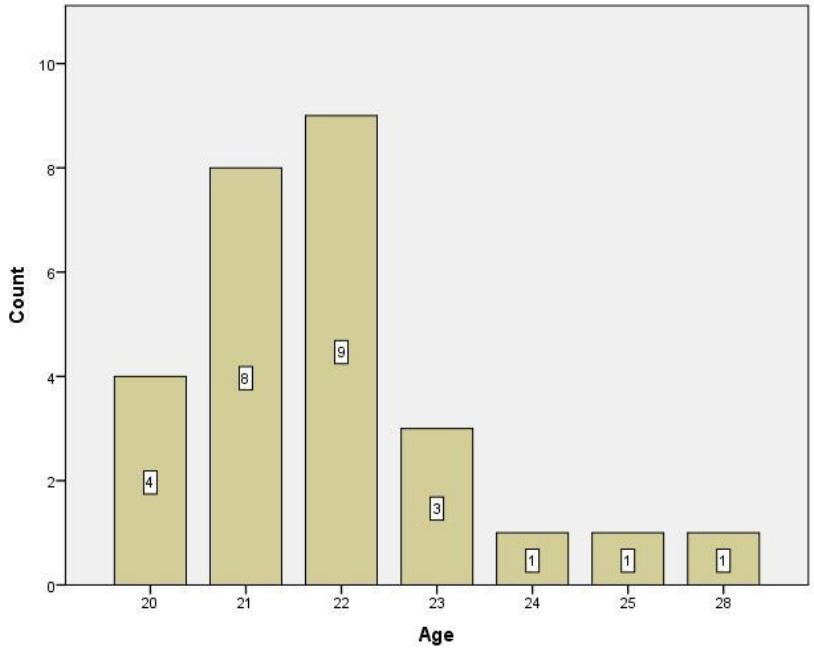
Figure 15: Final version of the thematic map

4.7. Results

4.7.1. Data sample characteristics

In this section, it will be presented some characteristics of the data that were collected in the closed questions of the questionnaires.

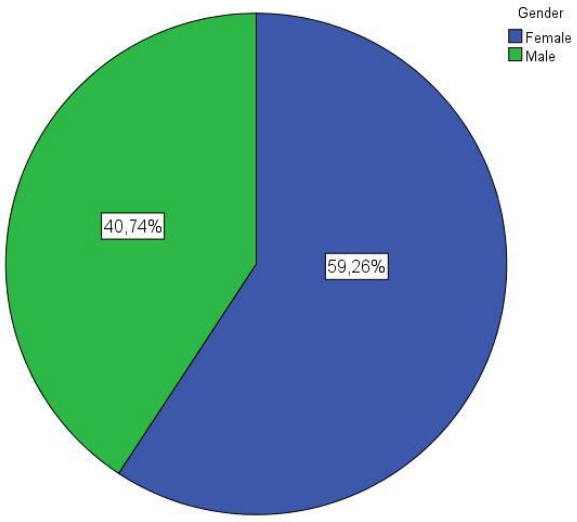
Graphic 3 illustrates the distribution of the participants of this experimentation per age. The ages of the participants are between 20 (twenty) to 28 (twenty-eight) years old.



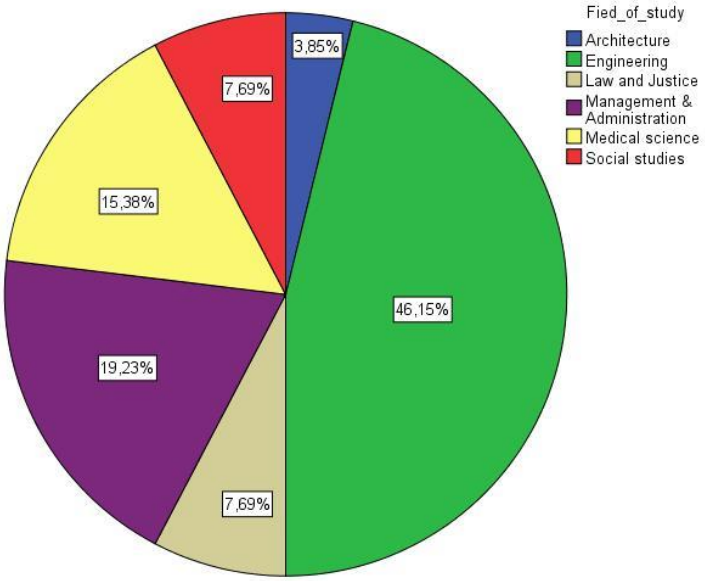
Graphic 3: Number of participants per age

Graphic 4 illustrates the distribution of participants of this experimentation per gender and Graphic 5 illustrates their field of study. The majority of participants (59,26%) are female and the remaining 40,74% are male.

Engineering is the field of study attended by most of the participants (46,15%), followed by Management and Administration (19,23%) and Medical Science (15,38%).



Graphic 4: Percentage of participants per gender



Graphic 5: Percentage of participants per field of study

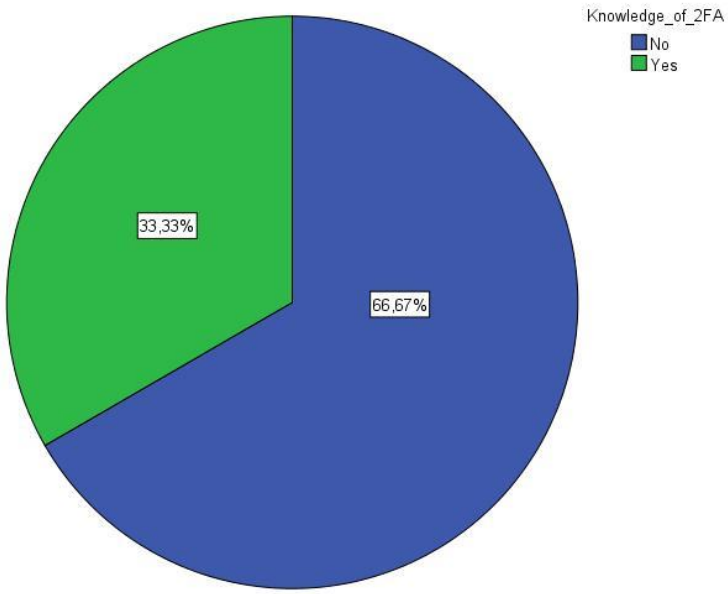
Table 8 shows the data collection about the users concern with the protection of their private information. The participants biggest concerns with their information is data access from unauthorized people followed by private/confidential data exposure from unauthorized people.

Concerns with private information	**Frequency**	**Percentage**
Fear that other people can access that information without authorization.	12	60%
Fear to see my private/confidential information exposed without authorization.	6	30%
I do not have any fears regarding private information.	1	5%
Other	1	5%

Table 8: Concerns with private information

The “Other” concern reveled by a participant is the improper use of the data that can make bad intentioned people (hackers) have access to information.

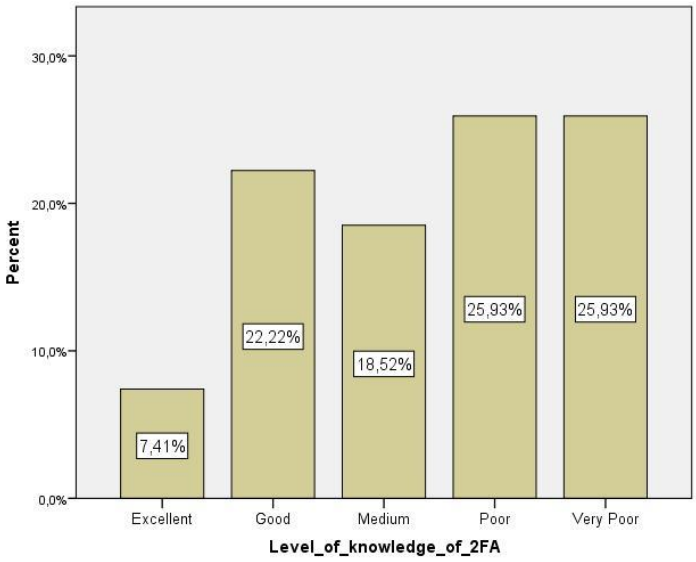
It is presented in Graphic 6 the percentage of users that were and weren’t familiar with 2FA before this experimentation. The results show that 66,67 % of the participants didn’t know 2FA while 33,33% were familiar with it.



Graphic 6: Knowledge of 2FA by participants before experimentation

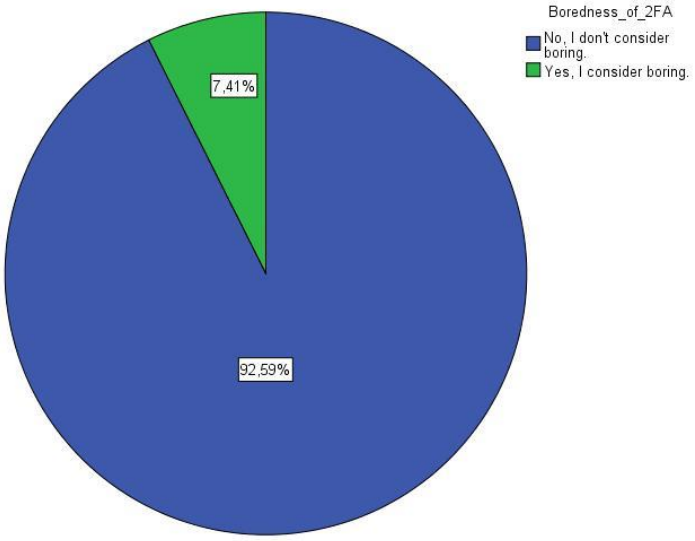
Graphic 7 illustrates the information collected on the knowledge about 2FA by participants before the experimentation.

They were asked to rate their knowledge on this topic from a scale of very poor to excellent. The results show that almost half of the participants have a poor or very poor knowledge about 2FA.



Graphic 7: Level of knowledge of 2FA of participants

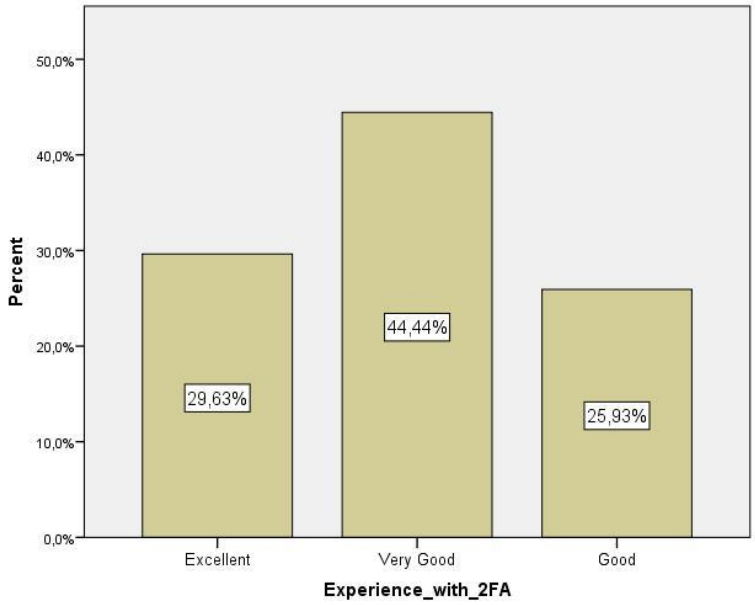
Graphic 8 presents the rating the users gave before the experimentation for 2FA boredness/troublesome. That is, if users consider 2FA boring to use or not. The results demonstrate that most of the participants (92,59%) do not consider 2FA boring/troublesome.



Graphic 8: Boredness of 2FA

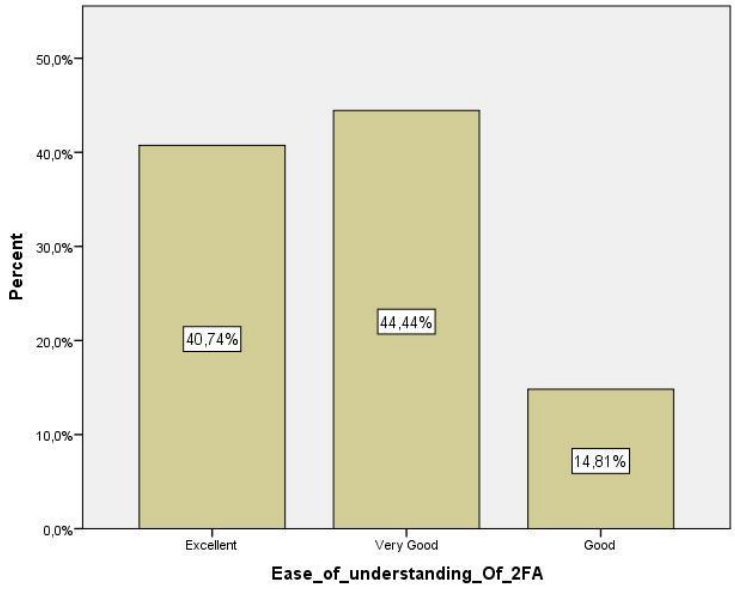
Graphic 9 presents the results of the rating of user satisfaction with 2FA by participants. With user satisfaction, we mean an aggregate of low boredness, ease of understanding of how it works and the security advantages that it presents.

As it can be seen in the graphics most of the participants (44,44%) consider that they have a very good experience when using 2FA, 29,63% consider that they an excellent experience while 25,93% have a good experience.



Graphic 9: Experiences of users with 2FA

Graphic 10 presents the results of the ratings of the ease of understanding on how 2FA works. 44,44 % of the participant rated their ease of understanding of how 2FA works as “Very good”. This means that, most of the participants have no difficulties in understanding how 2FA works.



Graphic 10: Ease of understanding of 2FA

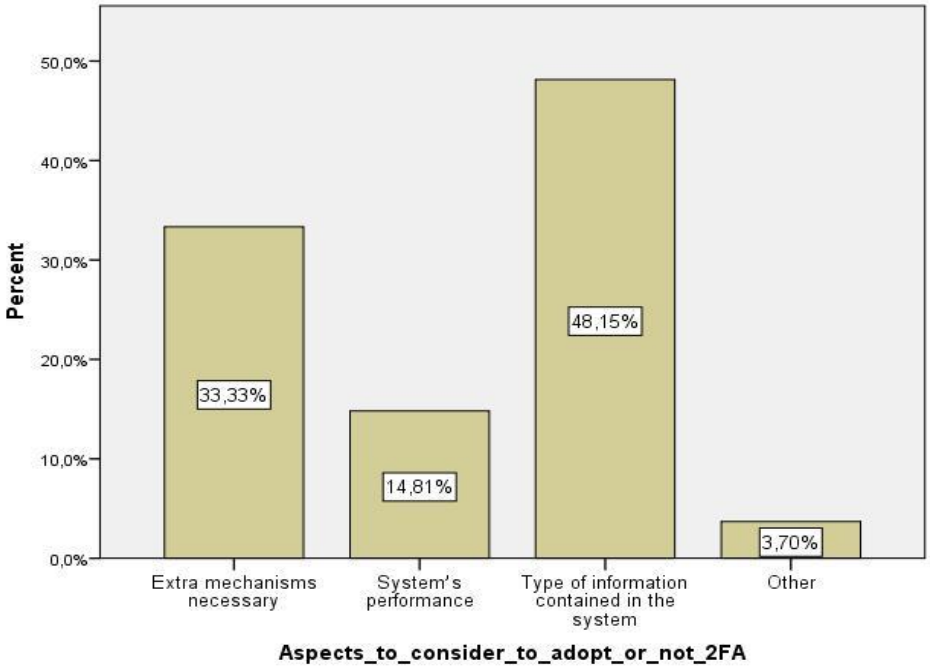
Table 9 presents the results of the participants opinion on the importance of the security increment that 2FA adds. That is, users were asked if they consider important the extra layer of security that 2FA offers. Most of the participants (62,96 %) consider that it is important.

Importance of the security increment that 2FA offers	**Frequency**	**Percentage**
Yes (It is important)	17	62,96%
No (It isn't important)	0	0
It depends on the type of system	10	37,04%

Table 9: Importance of the security increment that 2FA offers

Graphic 11 illustrates the aspects that the participants consider when deciding whether to use or not 2FA in their systems/applications.

The options were: Extra mechanisms necessary (such as smartphones, hardware token, access to email, etc), System's performance (meaning quickness or delay accessing a functionality) and Type of information contained in the system (public or private information).

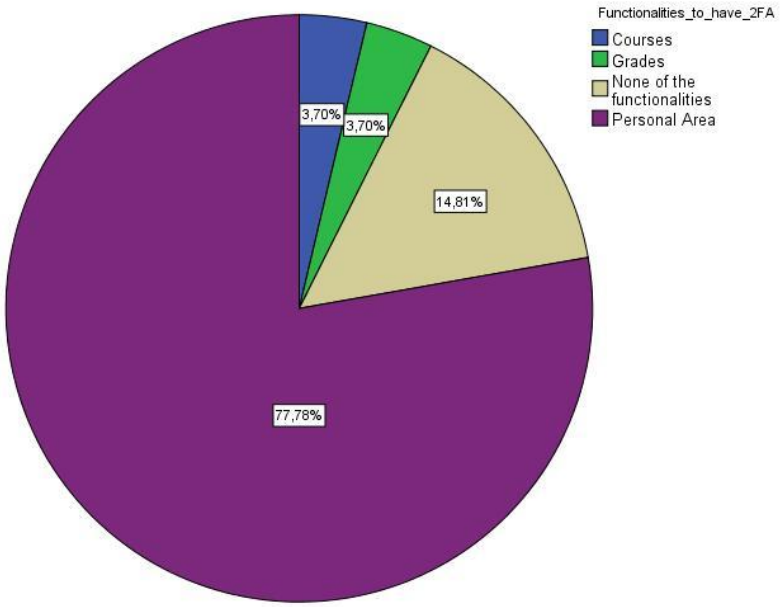


Graphic 11: Aspects considered by the participants to adopt or not 2FA

48,15 % consider the type of information contained in the system is the most important aspect when deciding to adopt or not 2FA, 33,33% consider the extra mechanisms necessary, 14,81% consider the system's performance and 3,70% consider other aspects.

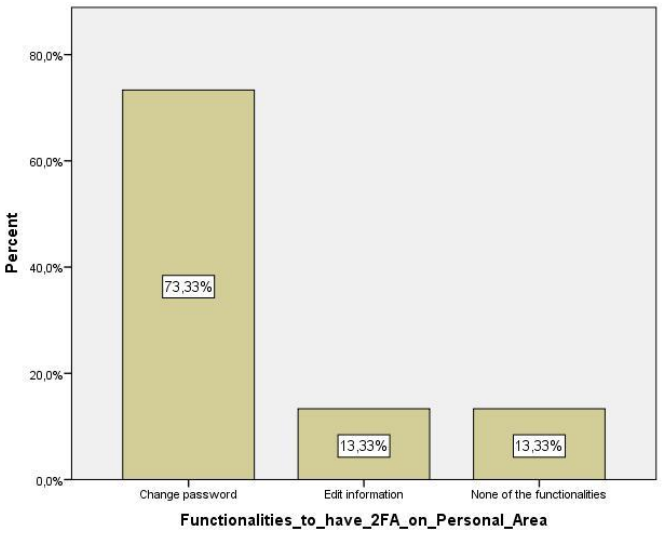
The participants that answered "Other" had the opportunity to specify which other aspects they consider. One participant answered "Other" and specified that he would consider the complexity of the system and if it is a critical system (involves money or not).

Graphic 12 represents the functionalities that the participants would rather have 2FA on it in an E-learning system. According to the graphic, most of the participants (77,78%) would choose to apply 2FA in "Personal Area" functionality. 14,81 % of the participants chose "None of the functionalities", 3,70% chose "Courses" and another 3,70% chose "Grades".



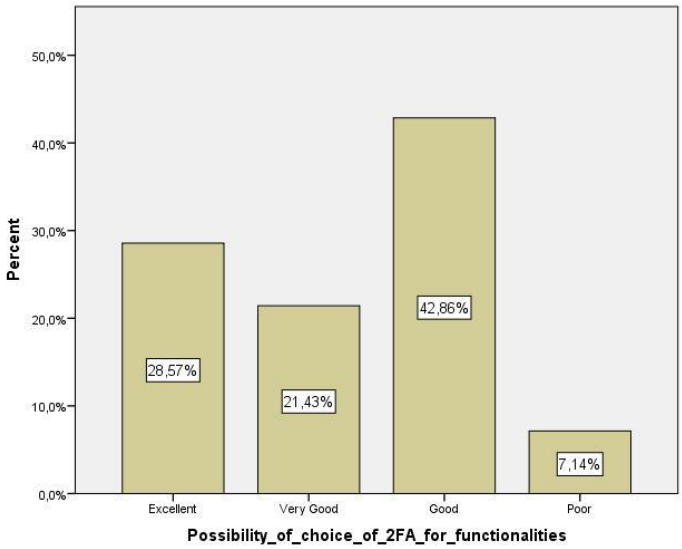
Graphic 12: Functionalities that participants would choose to apply 2FA in E-learning

The questionnaire also asked what sub-functionalities of "Personal Area" users would choose to apply 2FA. The results presented in Graphic 13 show that 73,33% would choose to apply 2FA to "Change password", 13,33% to "Edit information" and 13,33% would choose "None of the functionalities".



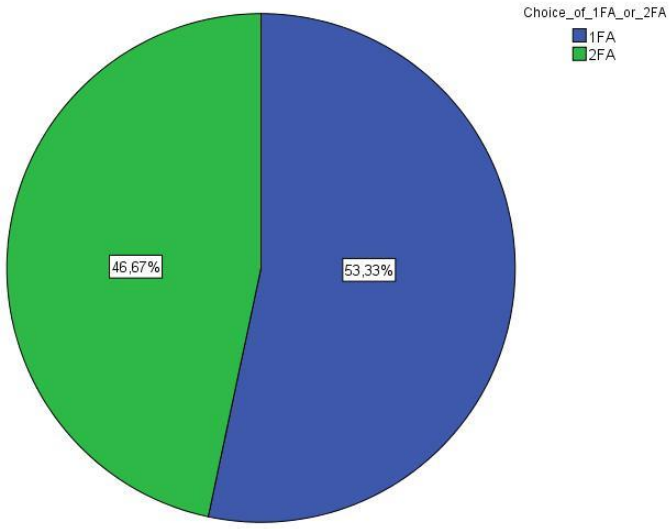
Graphic 13: Functionalities that participants would choose to apply 2FA in Personal area

The participants were asked to rate the possibility of choosing which functionalities of an E-learning system should have 2FA on it. Graphic 14 shows that most of the participants, represented by 42,86%, consider that a "Good" possibility 21,43% consider that a "Very Good" possibility, 28,57% consider an "Excellent" possibility and only 7,14% consider a "Poor" possibility.



Graphic 14: Possibility of choosing 2FA for functionalities of E-learning system

We also asked the participants if they would rather apply 1FA or 2FA in the functionality "Check balance and transactions" from a homebanking system. Since in this functionality is not mandatory to have 2FA, users had the possibility of choosing between 1FA or 2FA.
The results presented in Graphic 15 demonstrated that 53,33% of the participants would choose to apply 1FA and 46,67% 2FA.



Graphic 15: 1FA or 2FA for ''Check balance and transactions'' in homebanking

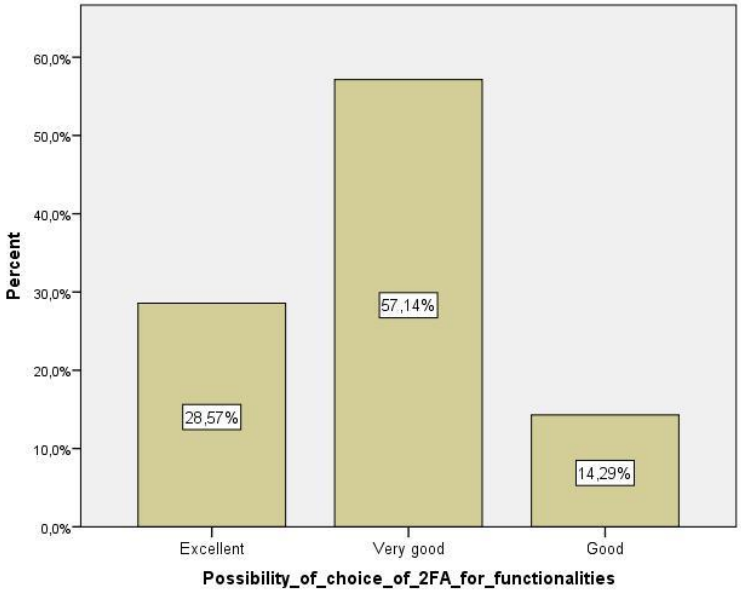
Table 10 presents the results of the participants preferences for having functionalities with mandatory 2FA or not having access to them. Most of the participants (95,24%) would still want to access a functionality with mandatory 2FA rather than not having access to it.

Have 2FA applied or not have access to functionality	**Frequency**	**Percentage**
I would rather have access to the functionalities with 2FA.	15	93,75%
I would rather not have access to the functionalities.	1	6,25%

Table 10: Users preference for having functionality with mandatory 2FA or not

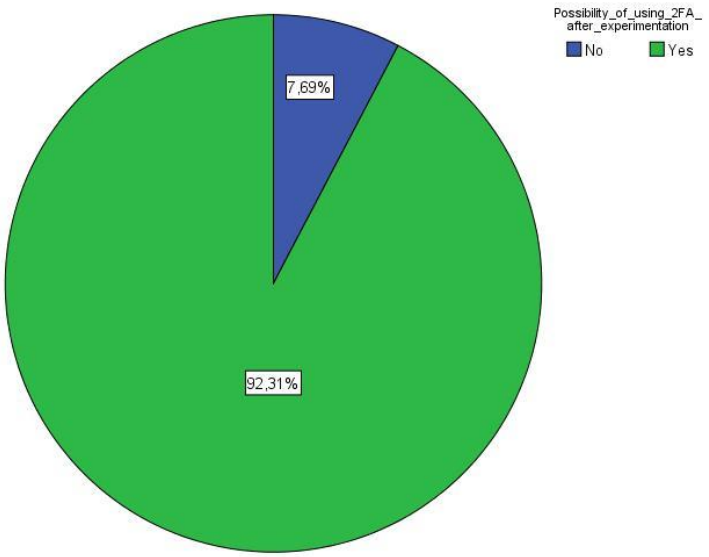
In the homebanking questionnaire, the participants were asked to rate the possibility of choosing which functionalities of a homebanking system should have 2FA on it. 57,14% consider a "Very

good" possibility, 28,57% consider an "Excellent" possibility and 14,29% consider a "Good" possibility. The results are presented in Graphic 16.



Graphic 16: Possibility of choosing 2FA for functionalities of Homebanking systems

At the end of the questionnaires we asked the participants if they would consider use 2FA in the application/systems that offers that possibility. Graphic 17 shows that 92,31% of the participants indicated that they would consider using 2FA after this experimentation.



Graphic 17: Intention of using 2FA after the experimentation

4.7.2. Thematic analysis results

From the thematic analysis that was conducted, important concepts were identified, and three themes emerged. These themes are: 2FA Disadvantages, 2FA Advantages and 2FA applied to functionalities.

Throughout the description of these themes we give examples of data extracts in order to support our argument regarding the results. There were aspects and considerations made by participants that go beyond the themes that were created and the scope of this dissertation. For example, when the participants were expressing their concerns about the disadvantages of 2FA they also suggested ways to overcome some of those disadvantages. This provides evidence of the participants interest in 2FA as well as their experience with this topic. However, these aspects will not be presented and analyzed since it is not part of the scope of this dissertation.

- **2FA Disadvantages**

This theme presents some aspects described by the participants with their experience with 2FA. By approaching this theme, we intend to present some aspects that the participants consider a negative facet of 2FA.

An aspect presented by many participants is the slowness that 2FA adds. This in turn, according to the participants, makes the process boring. They consider that 2FA makes the process of accessing accounts and/or functionalities slower given the fact that is necessary to introduce more than one factor.

These opinions were verified in several data extracts as shown below.

**: 2FA makes the process of accessing accounts slower.*

**: Most of the times I used 2FA I had a boring experience.*

**: 2FA is a little boring.*

**: I loose too much time doing some operations in my homebanking because it is mandatory to use 2FA.*

**: The disadvantage is the inconvenient of having to take one more step before accessing information.*

Another aspect that was mentioned by the participants is the fact that 2FA demands users to have "something that the users have" with them to complete the process. The participants consider this an inconvenient since if they do not have the second factor they cannot have access to the system.

**: 2FA might sometimes impose users to have a device with them (such as a smartphone in order to receive a notification by SMS). And if people don't have it they cannot access the system.*

*: *It is necessary to have "something that the user have" to be used as the second factor to access the system.*

Some participants consider that there are aspects that surround 2FA that need special attention. An important aspect described is if users change their cellphone number to where usually the code is sent or if for some reason they cannot access their email. In these scenarios users won't have access to a system/application.

**: It is important to give special attention when users change their cellphone numbers (used as second factor) or if their email is blocked for any reason.*

**: 2FA might cause people to be stressed in case they can't have access to an email at the moment that they need the code.*

- **2FA Advantages**

This theme characterizes the participants impression on the advantages offered by 2FA. It presents some key concepts of the best features of 2FA that were identified by the participants.

The participants were asked to describe some aspects of their experience with 2FA that they would want to mention. They mentioned the security offered by 2FA in systems, its importance to data confidentiality, and data protection.

Some of these aspects can be read in the following data extracts.

**: I think 2FA is very useful to ensure data protection especially in systems/applications that contain confidential data.*

**: 2FA decreases the probability of data theft.*

**: 2FA offers more security without wasting too much money.*

**: I believe that the main advantage of 2FA is the greater security of information that it offers.*

An aspect that was verified in participants responses was their opinion about the balance between 2FA disadvantages and advantages. Most participants consider that there might be some inconveniences while using 2FA (referred in the theme 2FA Disadvantages) however, 2FA offers an extra security by asking for more than one factor. They consider that although it can make the process slower, there are systems where it is necessary to have 2FA. And given that, participants consider that the disadvantages of 2FA are surmounted by the advantages that it offers.

**: 2FA gives more tranquility to users given the fact that security is greater than just using 1FA.*

**: I think that the advantages that it offers suppresses that inconvenient/boring side.*

**: Most of the times I used 2FA I had a boring experience, however, in some cases it is necessary to use it for security reasons.*

- **2FA applied to functionalities of systems (E-learning and homebanking systems)**

This theme characterizes the participants viewpoints on 2FA applied to E-learning and homebanking functionalities.

The participants were asked to give their opinion about their experience with 2FA in E-learning and homebanking systems, as well as, their opinion with their overall experience with 2FA.

Many participants considered very important to apply 2FA in homebanking systems because of the type of information that it contains. They consider that when it comes to systems that have money involved every measure to improve security is highly valued.

The data extracts below demonstrate the participants concerns with homebanking systems.

**: Having 2FA to access a system instead of having it for functionalities might be enough for some systems. However, in homebanking having 2FA for all functionalities is extremely important.*

**: When regarding the security of my bank data (specially operation with funds) every security measure that contributes to increase security must be considered.*

**: I consider homebanking systems extremely important to be as secure as possible, given that, it is important to have 2FA.*

According to some participants, every functionality that involves monetary transactions must have 2FA on it. Examples can be seen in the extracts below.

**: In homebanking, having 2FA in all functionalities that involves money transactions is extremely important.*

**: In homebanking systems, it is very important to have 2FA not only to login but in every functionality that involves monetary transactions and even to "check money and transactions".*

E-learning systems were evaluated by the participants as a system that is not critical to have 2FA because of the data that it contains. Although some participants showed some concerns to see their grades and personal information (such as cellphone number and address) exposed, most of the participants showed not having many concerns with applying 2FA in E-learning systems.

Some examples can be seen below.

**: In my opinion, an E-learning system is not something that needs confidentiality because it doesn't contain relevant data.*

**: It is good to have 2FA in E-learning systems because it offers greater security. It can be used in some functionalities of E-learning but not in all of them.*

Another topic discussed was the functionalities of E-learning that users would rather have 2FA on it. In this topic, different opinions were registered. Some participants don't consider important to have 2FA in any of the functionalities of their E-learning system while others consider important to apply in some functionalities. These functionalities are presented in some examples bellow.

****:** It would be good to have 2FA in functionalities such as login, to see grades and submit academic project.*

**: There are some information in E-learning that I consider that could be interest to have 2FA (such as personal information and grades).*

Some participants described some functionalities that in their point of view should only have 1FA.

**: In functionalities such as to access course materials there is no need to have 2FA.*

**: I think that functionalities such as video classes and other related functionalities can have 1FA.*

---

5. Discussion

5.1. Introduction

In this section, we present an analysis and discussion of the main results collected during the experimentations. Our findings are based in the quantitative and qualitative results. In many situations qualitative data was used to explain some of the quantitative results.
Furthermore, we make a comparison of our findings with other researches and describe some limitations of our study.

5.2. Main findings

The research conducted in this dissertation has as the main objective to discuss the impacts of the adoption of two-factor authentication (2FA) in users experience in terms of security and usability.
In an early stage of this research it was developed a general framework that had as objective to analyze/discuss the impacts of security policies and that could recommend the best one to a given organizational context.

In addition, we propose an approach where users have the possibility to choose which functionalities of a system should have 2FA on it. This approach was applied to two different scenarios: a university student web portal and homebanking systems. Some hypotheses were formulated, and a mix research was conducted to test them.

We present below an analysis of our results and the main findings related to the objectives that were proposed for this dissertation.

- **User awareness and acceptance of security advantages and disadvantages of 2FA**

During this research one of our objectives was to analyze user awareness and acceptance of security advantages and disadvantages of 1FA and 2FA.

In order to analyze users security awareness we tried to understand which aspects of information, that they consider private/confidential, worry users.

Users statements in the qualitative results have particular key words in common. These key words are ‘information security’, ‘data confidentiality’ and ‘data protection’. Almost every participant referred these words when describing 2FA advantages, disadvantages and the functionalities that they would want to apply 2FA on it. Moreover, based on the quantitative results, we could see that users biggest fear regarding information is that someone could have access to their private/personal information without their authorization. All of the participants of the experimentation consider important the protection of digital data.
With these results, we can conclude that users are preoccupied with information security and consider important to protect their digital data.

2FA is described by users as a mechanism that ensures the protection of confidential data in systems, and a mechanism that decreases the probability of data theft. As disadvantages, it was described the slowness in accessing functionalities, having as consequence a boring experience when using 2FA. Although some users referred in their statements that there is a boring side associated with 2FA, most users consider that in general 2FA is not boring and that they have a good experience while using it (referred in the quantitative results). This difference can be explained by the fact that when users describe textually their opinions they become more aware of the disadvantages than when they answer to questionnaires containing “Likert” scale. This also reveals that users adaptation to this mechanism has been increasing.
Those who had no experience with this mechanism, consider that, based on what they learned they expect to have a good experience with this mechanism.

- **Evaluating 2FA knowledge and adoption by users**

Our quantitative results demonstrated that most of the participants didn’t know what 2FA was until this experimentation. However, the results showed that most users considered that they gained more knowledge on this topic after this experimentation.

This demonstrates that we reached one of our objectives that was to improve users knowledge on 2FA and its related concepts.
There were participants that knew and had knowledge (at least a basic knowledge) of 2FA and there were participants that had never heard or had contact with 2FA. The responses of the participants that didn’t know 2FA until this experimentation were based in the Power point

presentation that introduced this concept and in the video demonstrating how this mechanism works.

2FA is optional for some functionalities/application. That is, users can turn on and off this mechanism, at any moment, in some functionalities/applications. Based in our results, we found that the number one aspect, that users think about, when considering to adopt or not 2FA is the type of information contained in the system. In other words, users want to consider if their system contains private and confidential information that they wouldn't want to see revealed, or if the information is public and/or there is no problem if it turns public. These findings are complemented with the fact that, as shown previously, users fear to see their private information exposed without their permission and the importance that they give to data protection.

- **Analysis of the implementation of 2FA in a university student web portal and in an homebanking system**

An important topic that we wanted to understand with this research is if increasing security of certain functionalities of systems would bother users, and if they understand the need for security in some systems.

Our qualitative study demonstrates that there are users who consider that, having 2FA to access functionalities in homebanking can make the process boring and slower, and can lead to a stressful experience. Despite that, users consider extremely important to have their homebanking system as secure as possible, given the fact that it contains sensible and important information. These findings can be complemented with the fact that in the quantitative results, most of the participants consider the security increment that 2FA authentication offers important.
With these findings we can affirm that increasing security of certain functionalities or systems might bother user activities. However, this inconvenient is well accepted by most users because of the security advantages that 2FA presents.

When we proposed the approach where users have the possibility of choosing which functionalities of a system should have 2FA on it we hypothesized that this would improve users experience with 2FA, because it would decrease the negative impact that it might have in user activities, and would also increase the adoption of 2FA.

We found that most of the participants consider this a very good possibility, both for E-learning and homebanking systems. At the end of this experience the majority of the participants considered to apply 2FA in the functionalities/systems that offer this mechanism. Unfortunately, we cannot affirm that 2FA adoption increased after this experimentation since we didn't have the opportunity to contact the participants to confirm this hypothesis.

Another observation that can be made from the results is that users consider that E-learning and homebanking systems should have different levels of security. In other words, although users consider that both systems should have 2FA in order to protect their information, there is clearly a bigger concern with homebanking systems. This concern can be verified in many data extracts provided in the qualitative results. In homebanking systems, most users argued that if they could, they would apply 2FA in all operations that include monetary transactions. A participant said that he considers important to apply 2FA even to operations such as to check balance. However, most users would rather apply 1FA to this functionality, as shown in the quantitative results.

- **User preferences for deciding between mandatory 2FA on a functionality or not having internet access to that functionality**

One of the aspects, that we wanted to analyze, was users preference for deciding between having a functionality with mandatory 2FA on it, or not having internet access to that functionality. As to the functionalities where 2FA is mandatory (represented in the homebanking interfaces as "Transactions" and "Payments") most users would still want to have access to that functionality with mandatory 2FA.

The idea of analyzing the choice of users for these two possibilities came after investigating a study where results showed that there was a user that canceled his bank account and switched to another bank because of the mandatory use of a hardware token (Krol et al., 2015). Although the dissatisfaction of the participant was with a particular 2FA technology an analogy can be made between these two aspects. In our study, a user (represented by 6,25% in the quantitative results) would rather not have access to the functionality than have it with mandatory 2FA.

- **Users preferences for functionalities that should have 2FA**

Since during the experimentation we gave users the opportunity to choose 2FA for certain functionalities, we analyzed users preferences for functionalities of E-learning and homebanking systems that they would rather have 2FA on it. That is, if they could choose which functionalities of those systems should have 2FA, what would their preferences be?

In E-learning systems most users would choose to apply 2FA in their "Personal Area" (as can be seen in the quantitative results).
"Personal Area" functionality also had sub-functionalities such as: "Edit information" and "Change passwords". We also wanted to analyze users preference for 2FA in these two functionalities. Most users would rather apply 2FA to change their password.
Important aspects can be extracted from these results, namely the importance of data protection that is referred in many of our findings. Applying 2FA to change password can be seen as a security measure that users take to protect against identity theft.

One aspect that can demonstrate users bigger interest with protecting systems that "as money involved" (as said by several users), is that the second option of users to apply 2FA on E-learning systems is "None of the functionalities". This means that, if users didn't have "Personal Area" as an option in the interface there are no functionalities that they would want to apply 2FA.

Users don't consider E-learning systems as critical systems. That is, systems that should contain high levels of security. Giving that, it is not so important to have 2FA in all of E-learning functionalities.

We asked users to enumerate more functionalities, that they would rather have 2FA and 1FA on it, besides of the options of functionalities that they had in the E-learning interfaces during the experimentation. In addition to "Personal Area", that was the choice of the majority of users, and "Grades" that was also one of the options in the interface, they proposed functionalities such as to submit academic projects.
Concerning 1FA users proposed functionalities such as: to access course material and see video classes.

5.3. Comparisons with past research

This research aims to discuss the impacts of 2FA in user activities in terms of security and usability. Previous studies have analyzed 2FA usability and security in general (De Cristofaro et al., 2013; Tsymzhitov et al., 2016), applied to homebanking (Weir et al., 2010; Gunson et al., 2011;Krol et al., 2015) and E-learning systems (Marton & David, 2015).

Users are aware of the impact of information security in their activities. In fact, all of the participants of this study consider important to protect their data. This awareness has also been shown in Montesdioca & Maçada (2015) research on users satisfaction with security policies. The results showed that users do understand the advantages of information security practices.

2FA is still unknown by many people. Most of the participants of this study did not have knowledge on this mechanism, before the study. This fact was also verified in others studies (Petsas et al., 2015; Ackerman, 2017). However, one of our objectives was to, if possible, increase 2FA adoption after this research.

Although we cannot state that we have increased 2FA adoption with this study, we could verify that most users demonstrated to have the intention to apply this mechanism in systems that offer this possibility. S. Ackerman (2017) made a research where, similarly to our research, in the beginning most of the users weren't familiar with 2FA. Their methodology was to show a video to users containing relevant topic of 2FA and, right after, that users would have to respond to some questions. They argued that, of their 90 participants, 31% consider 2FA a good and efficient solution and decided to apply it a week after. Their argument was that, when a message demonstrates the advantages, disadvantages, risks, and ways to overcome them, it can have a positive impact in users behavior. We consider that this argument also applies to our way of conducting the experimentation. Since we knew that not all of the users would know the concept of 2FA, it was important to give them some background. The participants considered that they increased their knowledge on 2FA after this experimentation.

We analyzed the aspects that users would consider when deciding to adopt or not 2FA. The authors of the previous described study also tried to understand the impediments for the adoption of 2FA. On the one hand, although our analysis was more focused on understanding the aspects users think about when considering to adopt or not 2FA, our results showed that users consider the type of data contained in the system (public or private) as the more important aspect for their decision. On the other hand, Ackerman (2017) research demonstrated that, most

of the participants answered that, the reason why they didn't adopt 2FA was because they were too busy to do it.

As to the case scenarios analyzed, E-learning and homebanking systems, there were verified both similar and different findings in comparison with other studies. On the one hand, Petsas et al., (2015) findings showed that in ebanking, users consider usability more important than security. In users opinion, there was no need for extra security in ebanking. On the other hand, our research found that users value the extra security added by 2FA and although this mechanism can be less easy to use, its advantages are perceived by users as necessary to a greater security of systems.

As to 1FA and 2FA analysis we found that, although 1FA makes the process of authentication easier, in homebanking systems users consider important to take every measure that improves security. The security increment added by 2FA is valued as an advantageous measure. Similar findings were described in a research that has as objective to analyze users perception of security and usability of 1FA and 2FA (Gunson et al., 2011). They found that 2FA is perceived by users as a secure solution however, it presents more inconveniences to the process (less easy to use).

Our results demonstrated that although it could be useful to have 2FA in E-learning systems it is not considered crucial to users. A study, that approaches some security considerations and 2FA opportunities in E-learning systems, argues that we live in an era where information is becoming more and more vulnerable, and because of that it is necessary to take measures in order to protect our private and confidential data (Marton & David, 2015). They add that this scenario can also be applied to students using E-learning systems where they can see their personal information shared.

Although most users consider E-learning not a type of system that they would apply 2FA in many functionalities, the results demonstrated that "Personal Area" functionality is perceived by most users as important to have 2FA. This choice by users goes along with Marton & David (2015) research work when regarding the protection of private and confidential information.

This research, as other research work (Petsas et al., 2015; Tsymzhitov et msal., 2016), demonstrated that 2FA is perceived as an advantageous mechanism to increase data protection as well as data/information theft.

5.4. Validity and limitations of the study

We collected 27 sample instances, from college students aged between 20 to 28 years old. Given this, the conclusions of this study can be made for college students that use E-learning and homebanking systems. Further studies are needed to determine if these results are the same for larges samples and with different age groups. This was a mixed study combining quantitative and qualitative analysis. We considered that 27 sample instances was acceptable to describe 3 theme instances, based on the tables of Fugard & Potts (2015).

During the experimentation, the moderator could unintentionally have had some interference in the participants opinions and consequently in their choices when answering the surveys. This could happen when users needed clarification about some aspect of the experimentation. The moderator made the necessary efforts to have a neutral position during the experimentations conducted.

6. Conclusion

6.1. Summary and contributions

The aim of this research, as described in this dissertation, is to propose a framework for discussing the impacts of IT security policies in user activities and apply the general proposed framework to a specific security policy (2FA) in order to understand the impacts of its adoption in user experience.

This dissertation proposes an approach where users have the possibility of choosing which functionalities of E-learning and homebanking systems, should contain 2FA associated. This option is perceived by users as a very good possibility and it increases their experience and usability, while using these systems, since they'll have the opportunity to apply 2FA in functionalities that they consider important to have this mechanism. However, this possibility does not apply to functionalities where 2FA use is mandatory, as imposed by some standards for certain functionalities.

With this research, users knowledge on 2FA and its related concept such as its advantages, disadvantages and security awareness have increased, and users presented interest in applying this mechanism in systems and applications that have this mechanism available, in the future.

This research provided important considerations about users perceptions of the advantages and disadvantages of 2FA, as well as, set of functionalities that users consider important to apply 2FA on it.

The next section identifies the objectives of this dissertation and describes how this research pursued them.

6.2. Objectives revised

In this dissertation we propose a framework for discussing the impacts of security policies in user activities. We, also, apply this general framework to a specific IT security policy (2FA) in order to understand the impacts of its adoption in user experience and to improve security awareness in the human resources of an organization

During this research, we pursued the following objectives:

1. Propose an approach to study the usability and security of 2FA in user experience in order to increase user awareness of internet security and experience with services provided by the internet.
2. Analyze the implementation of 2FA in a university student web portal and in an homebanking system.
3. Understand user preferences for deciding between having a functionality with mandatory 2FA on it, or not having internet access to that functionality.

We describe below how this research addresses the objectives presented.

- Propose an approach to study the usability and security of 2FA in user experience in order to increase user awareness of internet security and experience with services provided by the internet.

The methodology presented in this dissertation to study the usability and security of 2FA in user experience was to conduct experimentations with students that use E-learning and homebanking systems.

The first phases of the experimentation consisted in introducing to users the basic concepts of security and 2FA and to demonstrate how this mechanism work. In other words, we presented, discussed and analyzed 2FA to users since many of them did not know what this mechanism was or had little knowledge on it. This presentation, discussion and analysis were made in face-to-face sessions with users and by long-distance session when this discussion was made by exchanging messages with the participants.

The experimentation then proceeded to its next stages where users had to answer to questionnaires about their knowledge on 2FA and the two specific case scenarios we analyzed in this research: E-learning and homebanking systems.

The participants of this study were unanimous about the knowledge that they gained during this experimentation. The Power point presentation and the demonstration about 2FA were important for users to understand more about this mechanism and to answer the questionnaires.

The approach created in this dissertation (give users the possibility of choosing the functionalities that should have 2FA on it) increases users experience since it was perceived by most users as a very good approach and therefore, should be applied in systems.

Most participants demonstrated a clearly concern with data protection in their responses. They also demonstrated that they are aware of the risks associated with weak security measures. The results of the qualitative results present evidence of users biggest concerns with data protection.

The user awareness of the importance of information protection is a very important finding since it can demonstrate their commitment to protect data and consequently decrease the impact caused by the lack of security. Although many actions are still necessary to prevent attackers for stealing confidential information, users awareness is certainly a good step towards it.

- Analyze the implementation of 2FA in a university student web portal and in an homebanking system.

In order to analyze the implementation of 2FA in E-learning and homebanking systems two questionnaires were created (each one about one of the systems).

The results obtained allowed an analysis of the impact of 2FA in both systems, and about which functionalities users would rather have 2FA on it. In addition, users also proposed more functionalities that are usually present in E-learning systems that they consider it is important to have 2FA on.

2FA has an important role both in E-learning and homebanking systems. Both systems have functionalities that are important to be protected against impersonation fraud, identity theft, data theft, among other risks we are exposed to. However, there is a bigger trend to apply 2FA in more functionalities of homebanking systems than in E-learning systems. This trend is evidenced in many data extracts presented in the qualitative results.

Any system that has money involved is very important. This was stated by almost every participant of this study. The participants consider important to apply 2FA in every functionality that has monetary transactions associated. One participant considered that besides applying 2FA to functionalities that have monetary transactions associated, 2FA should be applied to check users balance and transaction.

In E-learning systems users are more concerned with having their personal information exposed without authorization. Given this, the most important functionality to have 2FA implemented in E-learning systems is “Personal Area”. Besides that, users do not have big concerns with their information in E-learning. A functionality that participants suggested that should have 2FA applied is to submit academic projects.

- Understand user preferences for deciding between having a functionality with mandatory 2FA on it, or not having internet access to that functionality.

During this research, we tried to understand users preference for deciding between having access to a functionality that has mandatory 2FA, or not having internet access to it. We tried to understand if 2FA presented such a burden that users would rather not have access to a functionality or if, despite the extra steps required, users would still want to have access to a functionality with mandatory 2FA.

In order to understand this preference, the questionnaires were prepared with questions that would enable us to make an analysis about this subject. Although some participants referred that 2FA might make the process of accessing an account or a system slower, users would still want to have access to a functionality with mandatory 2FA.

6.3. Future work

A proposal for a future study can be to contact the participants of this study, that were not familiar with 2FA and didn’t use this mechanism, and analyze its adoption and experiences in the early stages of its use after their participation in this experimentation.

In this dissertation, we gave users the opportunity of choosing the functionalities that they consider important to have 2FA on it. It would be interesting to add 2FA in some functionalities, that this study revealed as important to have 2FA, in a real system, and make an experimental study to analyze the impacts in user activities.

We also propose, as future study, the development of E-learning and homebanking systems that give users the option of choosing the functionalities to apply 2FA. That is, systems that have as a feature the option to turn on or off 2FA for certain functionalities (the ones where 2FA is not mandatory). For example, this study demonstrated that most users prefer 1FA to check their

balance and transactions in their homebanking systems however, there were people that would prefer to have 2FA. With this feature, users can apply 2FA to functionalities that they consider important. Some people could apply 1FA to check their balance and transactions, while others could apply 2FA.

We would also want to put in practice the general framework proposed in this dissertation that has as the main objective to analyze/discuss the impacts of security policies in user activities. We have proposed that this approach would recommend the best security policy given the organizational context, previous user experiences with those security policies and users expectations with those policies. A future study could be to implement this approach (in particular using machine learning tools) and test it in some organizations.

6.4. Closing remarks

Nowadays, we all have information that we consider personal/confidential, and that we would not want someone else to have access to it without authorization. Technology has been gaining strength and developing very fast, unfortunately attackers are taking advantages of this strength to perpetrate illegal action such as information theft. These actions can have tremendous consequences to organizations and users.

This research demonstrated that 2FA can be an effective mechanism to protect data despite of the inconveniences that it presents.

This research also contributes to the state of art with important insight about 2FA applied to homebanking and E-learning systems. So far, there hasn't been many studies addressing this mechanism in these specific systems. Moreover, giving the users the possibility to choose which functionalities should have 2FA on it, has proven to be an effective approach. This study enabled us to find out users knowledge on 2FA, what the advantages and disadvantages of this mechanism are to them, and some functionalities that users consider important to apply 1FA and 2FA.

To finish, I would like to borrow this phase from Stephen Northcutt: "Be aware that 2 factor authentication is not magic, rather it is a step in the right direction" (Northcutt, S., n.d.).