ABSTRACT

Title of Document:	RISK ASSESSMENT OF EMAIL ACCOUNTS: DIFFERENCE BETWEEN PERCEPTION AND REALITY.
	Merine Priscille Zinsou, Master of Science, 2012
Directed By:	Associate Professor Michel Cukier

The use of Internet is associated with a growing number of security threats. This thesis analyzes how users perceive the security of their email account based on the email account provider. With our study, we aim to contribute to the information security systems literature in three ways: First, by taking a more complete view on security online, and reviewing the concept of usable security, usability, human-computer interaction, trust and user perception. Second, by performing an analysis of providers of online services specifically emails. Third, by applying a renowned risk analysis method called Information Security Risk Analysis Method (ISRAM) for risk assessment. The ISRAM analysis revealed that Hotmail, Gmail and Yahoo email accounts have a medium risk level, while the reality analysis demonstrated no clearly more secure account provider with only low level risk counts.

RISK ASSESSMENT OF EMAIL ACCOUNTS: DIFFERENCE BETWEEN PERCEPTION AND REALITY

By

Merine Priscille Zinsou

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Master of Science
2012

Advisory Committee:
Associate Professor Michel Cukier, Chair/Advisor
Professor Ali Mosleh
Professor Mohammad Modarres

Acknowledgements

I would like to express my appreciation to my advisor, Michel Cukier, who introduced me to this new field of Reliability Engineering and believed that I could succeed in it. I would also like to express my gratitude to the committee members, Dr. Ali Mosleh and Dr. Mohammad Modarres for their helpful feedbacks on this research. I want also to thank my family for their support and continuous encouragement. To all my friends, you helped me move forward every time I was stuck and I am very grateful. A special thank you to all the people I met during my fellowship in Nanjing University of Science and Technology, China and also during my internship at Pratt and Whitney Rocketdyne, Florida. You helped me understand the importance of my chosen field of study.

Table of Contents

Chapter 1: Introduction

1.1 Context

Cyber security is gaining a lot of momentum lately with many attacks happening globally. Whether called information security, computer security or cyber security; one of the main challenges is to protect data that are personal, private, and sensitive in nature. Sample recent incidents include a 31-year old man who pleaded guilty to a $ 1.3 million phishing scam in Atlanta Georgia; a UK man who was sentenced to one year in prison for hacking Facebook accounts. Kaspersky, one of the fastest growing IT security companies worldwide, found that 600,000 Mac computers were infected with a Flashback Trojan, a malware program designed to capture user information for the purpose of fraudulent activities [9]. In June 2012, a Cybersecurity News blog affirmed that the FBI reported arresting twenty four people in four continents within two years for credit card fraud and banking crime [3]. In addition, the Government Accounting Office (GAO) reported a 19% increase in federal data breaches in July 2012 [4]. These alarming stories and reports clearly indicate that there is still more to do to control and minimize cyber criminality.

Humans are indispensable in any communication network; yet many researchers have proven that humans are the weakest link in the security system [18, 22, 28, 36, 52, 57, 65, 67, 69, and 75]. The behavior of the user as a potential source of security breach was studied by these various researchers. Liginlal et al. [28] in 2008 study the causes of privacy breaches with an emphasis on human error using GEMS (Generic Error Modeling System) error typology and publicly reported incidents. This 2008 study categorizes errors as slips and mistakes. The authors found that the most common form of human error related to privacy breaches were mistakes at the information processing stage of information system. Kraemer et al. [69] studied human and organizational factors and their interactions within Computer and Information Security (CIS). Based on their studies, in 2011, Kraemer et al. presented a model for threat detection which includes judgment, decision-making and learning theories [69]. Human errors can lead to vulnerabilities. In 2005, Ghi et al. proposed an elaborated taxonomy based on the 1993 taxonomy of Baskerville which develops the role of human error in security risk [36]. The initial study, the 1993 taxonomy of Baskerville, was based on threats published in the "Risks to the Public" column edited by Peter Neumann in Software Engineering Notes for a two-year period while the new and elaborated study was based on the newsgroup publications that actually caused damages to people and organizations. Both studies classify the threats in two major fundamentally opposite classes: accidental and deliberate. Furthermore, they redefined the "human error" threats as skill-based slips, rule-based mistakes and knowledge-based mistakes.

On the other hand, many other researchers studied the attackers' perceptions based on the security system in place, legal consequences, Internet Service Provider (ISP), firewalls and Intrusion Detection Systems (IDS). One way attackers' behaviors were modeled was using behavior based attack graphs [62] and another way was by building a profile following a remote compromise [25]. In addition, Holt and Kilger studied attackers' willingness to attack critical infrastructure both online and offline. They reported, in an article based on a study done at the University of Michigan, that cyber attackers who are likely to attack the government are also capable of illegal online activities [7]. In 2012, countermeasures were also examined to analyze their effects on attackers' intentions to hack a system [40]. While attackers' behaviors are important in determining the threat level in information security, the users' behaviors are equally as important in determining the threat level in information security.

1.2 Issues

The openness of the Internet makes it difficult to control. Internet users are limitless in their activities and some are malicious. While most cyber attacks are launched against high value targets such as government, banking institutions, CIA and FBI, there are also cyber attacks against a regular user or individual. These are often due to the individual's carelessness, mistrust or ignorance. The user thus becomes an important characteristic of information security. Consequently, minimizing cyber security incidents or avoiding them start with individual responsibility. Many situations may arise where the user quickly closes a connection without logging out of their accounts, closes a page without signing out. Other instances include a situation where users write down important login information on a sheet of paper, which they misplace or situations where the users are victims of social engineering. Social engineering is the art of convincing a user to be a person of trust in order to gain their personal information or information about others. Universities are full of young students who represent a perfect target for cyber attacks since most college students received emails from their peers, from potential employers and also they heavily used social media.

1.3 Approach

Our approach in this study is an attempt to apply reliability methods to information security. We will start by examining different free email providers based on their security and perform a comparison of their features. Then will follow a risk assessment of the information security system as perceived by some students of the University of Maryland, College Park.

The reality analysis will allow us to examine and possibly classify the email providers based on their security parameters and users account protection levels. In addition, the perception analysis will be based on a well-known risk analysis method called Information Security Risk Analysis Method (ISRAM). A final comparison will then be made between the results of the reality and the perception analysis to put in evidence their differences and similarities.

1.4 Contribution

Students of today will be the workers of tomorrow and will constitute a higher barrier to cyber attacks if they are aware of these problems early and regularly take steps to protect themselves and their institutions. In addition, our study will be an application of a well known reliability quantification method in information security which includes the user. Also, this study will help evaluate the security of users with free online email accounts.

The goal is to analyze how users perceive the security of their email account based on the domain in which it was created. For instance, is a student in a university more confident about their .edu account compared to a .com account? Are some of .com accounts more trustworthy than other? Does the reputation of Yahoo, Google, and AOL or university information technology services matter? This research is important because it will help information security managers identify the weaknesses of the account they provide based on the users' perception. It will also show whether training or awareness programs are needed to prevent attacks of email accounts or protect users' information.

With our study, we aim to contribute to the information security systems literature in three ways: First, by taking a more complete view on security online, and reviewing the concept of usable security, usability, human computer interaction, trust and user perception. Second, by performing an analysis of providers of online services specifically emails and third, by applying the steps of a renowned risk analysis method for risk assessment.

1.5 Outline

In chapter 2, we review the relevant literature on information security, human computer interaction, usability, web-based information systems, trust, secure communication and user perception. We describe a study in which user's perception is analyzed in terms of security and authentication purposes; then we review some studies on email accounts. We conclude the related work chapter with a summary of the literature with facts that pertained to this research.

The rest of the thesis is organized as follows. In chapter 3, we discuss a general overview of the email account providers and the risk analysis method used in the reality analysis. Based on this overview, diverse perspectives are integrated into a summary of characteristics for the risk classification and the risk analysis.

In chapter 4, we identify the elements that are pertinent to the perception analysis and conduct the risk analysis. Next, a table summarizes the results of our survey. The perception analysis section concludes with a ranking of the different providers.

Chapter 5 concludes the thesis with a discussion, where we point out the difference between reality and perception, the limitations of the present study as well as directions for future research.

Chapter 2: Related Work

There are two general bodies of research relevant to our work in information security. On the one hand, there are human factors, types of human errors and their management, and on the other hand, there are human-computer interaction, usability, web interfaces, user perception and some factors that affect perception such as trust, quality, loyalty, and satisfaction.

2.1 Understanding information security

2.1.1 Roots of human error in information security

Many researchers who study human error in security have speculated about the roots of system design problems. Vu et al. in 2010 [51] studied the use of a privacy bird figure that would change to different colors to warn the user about the potential threat of a computer program. The users' confidence levels were increased with this method and they adopted better privacy practices when using different websites. Maxion et al. [65] found that complicated user interfaces leading to a longer search for the correct information by the user are usual causes of human error. The authors proposed an alternative design that was proven to facilitate response and reduce response time. Perkovic et al. [75] found that security system design flaws are the root of non-uniform behaviors of users in security and difficulties in authentication that help attackers break into system. Design flaws also include the choice of password schemes used in information security authentication. Graphical passwords were proposed as a replacement for text passwords; however, these were often unsecure because the attacker could more easily guess the password, or the users found them difficult to remember or wrote them down.

Davis [26] and Thorpe [49] studied the effectiveness of some graphical password methods. Thorpe et al. found them “as susceptible as traditional text passwords” while Davis et al. proposed their own “Story” scheme, which they proved to be more effective than the “Pass-face” scheme; the pass-face scheme uses recognition of human faces instead of words for authentication. Cranor [52] defined a framework that could help system designers identify the causes of failures caused by humans, and also design a better system that incorporates human behavior and error. Boyce et al. [57] in 2011 examined how human performance affects cyber security. They defined four areas of concern for an effective cyber security system:

- usability and security compliance
- mitigation of human error and risk reduction
- enhancement of situation awareness
- development of effective visualization tools and techniques

This definition encompasses all the different issues approached by the previous researchers. Boyce et al. proposed a two-step process for mitigating human error. First, there is a need to find all the tasks associated with information security that the user performs and, second, with task modeling, ways must be found for tolerating those human errors as well as incorporating the human in the system with Human Systems Integration (HSI). Some studies present taxonomies for including human factors in security designs and implementation. Ghim at al. [36] developed steps that could help in evaluating the consequences of human error in information security. Kraemer et al. [68] proposed “a conceptual framework for examining human and organizational factors contributing to computer and information security.” Likewise, Moller at al. [70] proposed three steps: simulate potential user behavior, predict user behavior and design intended user behavior.

2.1.2 Human reliability and information security

In attempting to apply human reliability to information security, previous work has focused on the inclusion of human error in information system management. Cheng et al. [22] proposed a model in 2006 that used probability risk assessment applied to human behavior. Their methodology was to classify the potential faults in a system, define human error and quantify Human Error Probability (HEP). HEP is defined as “counts of misplay/counts that may happen” In their model, the authors did not use any known model of human reliability but the basic probability definition. The limit in this model was that data for the calculation of HEP is not readily available in real life. Thus, the model’s focus was on the policies, regulations, training and system design that could help minimize or prevent human error.

Many other studies such as Schultz et al. [30] in 2001 did not focus on quantifying the effects of human factors in information security. Rather, they developed the possible threats to information security, the different types of user errors and risks and suggested ways of resolution. Categories of user behavior found by Schultz are user performance, user acceptance or resistance of security methods. In contrast, Parkin et al. [73] in 2009 estimated human risks as “intentionally malicious,” “knowingly unsecured,” and “sources of accidental breaches.” A model assessment framework for analyzing cyber security was defined by Sommerstad et al. [74] in 2009. The authors used “different architectural scenarios based on Bayesian Statistics and external influence diagrams to express attack graphs and related countermeasures.” The goal was to quantify the probability of a successful attack as was attempted by Ralston et al. [61] in 2007.

2.1.3 Human factors and information security threats

Many studies have found human failure to be the cause of information systems security breaches. The behavior of the user confronted by a security system is often the main concern when evaluating faults. Thus, Khidzir at al. [59] attempted to determine the information security risk factors categorized as threats and vulnerabilities. They found “the most critical vulnerability is insufficient attention to human factors in the system design and implementation.” Similarly, in 2009, Liginlial et al. [28] found most cases of privacy breach incidents to be from human mistakes. They proposed a strategy based on error avoidance, error interception and error correction. Probst et al. [23] studied the effects of insider threats within an organization. The research found that trust is an important aspect of insider threat but difficult to model into security systems. The motivation and intent of the users are other aspects that can affect security; however, since human behavior changes over time, the authors found it difficult to predict the reliability of the user and thus detect the attacker’s behavior. But, in 2009, Colwill [18] determined human factors and themes that could help assess and manage the insider threat to information security.

Few researchers focused on quantifying human performance reliability in cyber security and incorporating human factors into information security management/assessment. In 2009, Kraemer et al. [69] categorized human and organizational factors in nine areas and examined their effects on computer and information security vulnerabilities. Askren et al. [78] proposed ways of computing human performance reliability for tasks in the time-space continuous domain in terms of time-to-first-error following a Weibull distribution, time-between-error following a log-Normal distribution, and time-to-error-correction also following a Log-Normal distribution. In 2008, Colombo et al. [67] proposed an Integrated Recursive Operability Analysis (IROA), which includes human and organizational factors into safety analysis based on previously developed Recursive Operability Analysis (ROA). Trcek et al. [27] developed a template model to aid the risk management for information systems based on human factors using business dynamics. Islam et al. [71] proposed a methodology that is composed of: identifying human factors in security risk management; categorizing them based on individual, team management and stakeholders; conducting a risk identification, analysis and mitigation. Finally, the authors developed a framework for incorporating those factors into the secure software architecture.

Additionally, in 2010, Khan et al. defined cyber security as a “whole set of procedures and systems providing protection of computer systems and network” [53]. For cyber security management (“predictive calculation of cyber attacks occurrence” [53]), the authors based their calculation on cyber attacks that are discrete events. They developed a customizable model for the quantification of cyber security for which the metrics are risks, vulnerabilities, threats, attacks, consequences and reliabilities. Each of the metrics has its own distribution and model. The risk is the final metric, which is a factor of vulnerabilities, threats and consequence used for analysis. This model is the closest to our experiment in the attempt of calculating risk. However, the quantification involves many parameters and different distributions: the data for the distributions assumed are not available for our study, and this methodology is also a composite of many mathematical equations that make it difficult to reproduce.

2.2 Human Computer Interaction

From a computer science perspective, HCI deals with the interaction between humans and computers; it should enhance the “user friendliness” of a system [46].

2.2.1 Human computer interaction and security

Computer users are exposed to technology mainly through user interfaces. Most users’ perceptions are based on their experience with these interfaces. Johnston et al. [46] focused on the aspects of Human-Computer Interface (HCI) that related to information security and called it HCI-S. HCI-S is defined as “the part of a user interface that is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security.” [46] The authors defined six factors that were taken from the ten criteria for a successful HCI described by Jakob Nielsen, one of the main researchers in the field of HCI. For a good HCI in the area of security, some criteria (convey features, visibility of system status, learnability, aesthetic and minimal design, errors, satisfaction) are essential. In addition, after implementation of all these criteria, the interface should lead to trust by clearly informing the user of the risks and how these risks can be minimized. Fostering trust with a high-quality interface that projects quality and professionalism will increase HCI-S. Trust in HCI-S is “the belief or willingness to believe, of a user in the security of a computer system” [46]. The goal of HCI-S is to create a robust, reliable and more secure system by making the user interface as friendly and intuitive as possible. This idea is interesting but it only stops at the design stage, while human computer interaction does not stop after the design is complete.

2.2.2 Human error and HCI

The other part of HCI that HCI-S does not cover is that a well-designed interface can increase productivity and reduce human error. A definition of HCI that includes productivity and the possibility of error is “the part of a computer program responsible for establishing the common ground with a particular (i.e., well-known) user. Such task is accomplished by expanding and maintaining this common ground throughout the interaction process with the application. Whenever possible, direct manipulation of familiar objects should be the leading interaction principle.” [46]

The shortness of this definition of HCI, however, is that it deals with a particular well-known user. However, there is no capability of knowing a particular user of a system as it goes on the market or outside the production field. Users could range from expert to novice to a person with disabilities to college student or to a merchant. All of these users have different knowledge of computers and computer systems and, thus, “the interface needs to ensure that the user is guided, so as to minimize the potential for the user to be the weakest link.” [46]

There is a need for user-interface designers to understand the common types and causes of human error, and the ways in which they may be prevented. When interfaces are designed to eliminate the conditions that lead people to make mistakes, interfaces will be more dependable, and the applications they serve will be more secure [65]. Maxion et al. [65] showed that goal errors that are "the failures of users to understand what to do" were a common type of error. They designed a method called ESS (External Subgoal Support) for user interfaces that prevented the reoccurrence of an error and proposed a solution to the specific issue of goal errors [65].

Furthermore, Abascal et al. [50] investigated inclusive design guidelines for socially and ethically aware HCI. The authors focused on the important role played by HCI in the provision of social opportunities to people with disabilities. A previous way disability workers have tried to cope with unfitted HCI was adapting commercially available computers to the capabilities of users with disabilities. Nevertheless, some drawbacks were the lack of generality, because users had different characteristics; and the dependence on current technology, but as the new technologies arrived their efforts became obsolete [50]. The second approach was the application of HCI paradigms to assistive technology by creating independence between the interface and the application and using advanced user interface design techniques. In that sense, Hervas et al. [64] pursued an automatic user interface generation process: the ViMos framework, which is an infrastructure to generate context-powered information visualization services dynamically in which the designer does not need knowledge on programming or design. Only detailed knowledge on the application domain is required to specify the context model for visualization. In addition, users need to define the personalization of the information they desire [64]. This interface generator will enable the view of “the right information to the right person in the right place” [64]. Therefore, this proposal only affects information presentation and combines semantic web languages, adaptability techniques and well-known design patterns [64]. Moreover, there are a great number of issues to consider when designing a user interface that ViMos manages and with the general user context, generates the user interface at run-time [64].

Adding to the interface properties, Abascal et al. [50] suggested that interfaces should be aware of users’ needs and proposed guidelines for HCI designers. The problems of HCI can be overcome with international collaboration, standardization and legal protection [50]. Johnston et al. also agreed that policies are needed for making the most practicable interface utilizable [46].

2.2.3 Usability and HCI

Usability is often considered as a part of HCI. For instance, Teo et al. [43] listed reduction in number of errors, enhanced accuracy, more favorable attitude towards target system and increased usage as correlated to usability. The authors in [46] asserted that usability can be implemented in HCI for security systems using their predefined criteria mentioned earlier. Moreover, when tasks are completed “easily, effectively and efficiently,” usability plays an important role in HCI [50]. Consequently evaluating user interface is necessary for attaining usability [43].

When assessing user interface for usability, there is the notion of interactivity. Interactivity “is the degree to which participants in a communication process have control over, and can exchange roles in their mutual discourse” with two key features: user control and information exchange [43]. The factors that influence the interactivity level are website purpose and interactive functions, but also user characteristics [43]. Many researchers used the level of interactivity with a website or the web interface characteristics to define the level of usability. In fact, Teo et al. reported six benefits of interactivity, namely, sense of fun and satisfaction, engagement, performance quality and time saving [43]. These could be completed by the six factors of HCI-S proposed by Johnston et al. and they convey features and visibility of system status, technology, convey features, aesthetic and minimalist design, learnability and brand [46].

2.3 Usability

Usability, in the field of Human-Computer Interaction (HCI), is widely defined according to ISO 9241-11, 1998 as ‘‘the extent to which a product can be used by specified users to achieve specific goals with effectiveness, efficiency and satisfaction in a specified context of use’’ (15, 12). Another definition of usability, in the field of Software Engineering (SE), according to ISO 9126-1 is ‘‘the capability of the software product to be understood, learned, operated, attractive to the user, and compliant to standards/guidelines, when used under specific conditions.’’[12] Teo et al. [43] defined usability as “whether the users can actually work the system successfully.” Many other authors [50, 12] agreed that users need to perform the tasks they wish to do easily, effectively and efficiently; usability is defined as such.

2.3.1 Universal usability

Two studies in the year 2000 defined universal usability, one at the usage stage, and the other from the design to usage stage. “Universal usability can be defined as having more than 90% of all households as successful users of information and communications services at least once a week” [16]. In this definition, usability is accessed based on success in utilization of information and communications services and frequency of use. Other authors stated that universal usability is “a focus on designing products so that they are usable by the widest range of people operating in the widest range of situations as is commercially practical” [39]. Here, usability should be designed into products and be appropriate in different domains.

A comparison of these two studies reveals interesting facts in the concept of universal usability. Shneiderman [16] lists three challenges in attaining universal usability, namely, technology variety, user diversity and gaps in user knowledge. In addition, Vanderheiden [39] developed a prioritization order for designing to universal usability: first, an analysis of accessibility/usability using 3-level features; second, assess independence/co-dependence; and third, an efficiency and urgency requirement with at least three factors, namely, the reversibility of the action, the severity of the consequence for failure and the ability of the person to adjust the time span to meet their increased reaction times. Another “pseudo-priority dimension” [39] added is ease of implementation.

Universal usability studies are gaining momentum as the Internet and technology are evolving [16, 39]. The four major objectives required to implement more flexible universally usable interfaces are: ensuring that all information presented by or through the device can be perceived even if all sensory channels are not available to the individual; ensuring that the device is operable by the user even if the device is operating under constraints; facilitating the ability of the individual to navigate through the information and controls even if they are operating with constraints and their ability to understand the content[39]. Moreover, Hochheiser et al. defined universal usability statements as “declarations by Web site designers of the usability measures and concerns associated with a given Web site. The statements describe the contents of a site, browser requirements, network requirements, and other characteristics that may influence its usability.” [42]

In a way, universal usability is difficult to assess on the web because it involves first multiple web pages with different levels of usability and accessibility, second diverse users with different perception therefore it becomes difficult to quantify universal usability [66]. These studies provide important insights into the usability of web services. However, what drives users to choose one site over the other?

A comparable analysis to email switching [37] hints that the availability of attractive alternatives, satisfaction and switching cost might impact users’ choices of websites; nevertheless, there is yet no empirical evaluation to validate the assumption.

2.3.2 Usability factors

Teo et al. expressed the web usability factors as the website’s learnability, throughput, flexibility and user’s attitude towards the website [43]. Teo and his colleagues defined attitude as “predispositions to respond in a particular way towards a specified class of objects” [43]. In a similar manner, Flavian et al. [19] listed five factors of website usability. The first and second factors pertained to the website characteristics that the user can see; the ease of understanding the structure of a system, its functions, interface, and contents observed by the user and the simplicity of use of the website in its initial stages. The last three factors relate to what the user can accomplish; the speed with which the users can find the item the user is looking for, the perceived ease of site navigation in terms of the time required and action necessary to obtain the desired results and the ability of the user to control what he/she is doing, and where he/she is, at any given moment [19]. However, the Roy et al. [54] analysis accentuated the interface's characteristics more than the users' actions. Hence, ease of navigation with user guidance and support improve the users' learnability, efficiency and effectiveness while consistency, learnability and perception target the website interface characteristics. Consistency relates to standards and conventions applicable to all websites in general; learnability implies a simple clear logical and well-presented design; perception or perceptual limitation aims to design an interface taking into account human perceptual organization limitations [54]. Overall, the authors' main concerns were the design of an interface with good characteristics as defined and the design of an interface suitable for its users.

2.3.3 Usability evaluation methods

Fernandez et al. defined the usability evaluation method as "a procedure which is composed of a set of well-defined activities for collecting usage data related to end-user interaction with a software product and/or how the specific properties of this software product contribute to achieving a certain degree of usability." [12] They further defined two classes of usability evaluation methods: empirical methods, which required participation from the real end-users, and inspection methods based on the views of experts and designers. In the software domain, Holzinger [13] designated empirical methods by test methods. The author recommended a combination of the two methods when testing for usability [13]. On the other hand, there are many other usability questionnaires/checklists such as Quis by Norman and Shneiderman, 1989; Sumi by Kirakowski and Corbett, 1993; PutQ by Lin, Choong and Salvendy, 1997; PSSUQ by Lewis, 2002; seLearn [15, 14] including Li et al. 2002 [15] available for usability evaluation.

2.3.4 Usability and security

Usability and security are competing features, noted in Gunson et al. [60]. Usability needs to be universal, based on the laws (Section Section 255 of the Telecommunication Act and Section 508 of the Rehabilitation Act [39] for example), libraries [16] and the rapid growth of Internet. Security, in contrast, aims at preventing access to every person other than the designated user. Yet, in the human computer interaction domain, usability and security often come together. Users are then confronted with security decisions that, if not well understood, can jeopardize their security [24]. It is necessary to design systems that are as usable as they are secure [24] by optimizing the liaison between the two [29].

Whether termed information security usability [29], usable security [24], it is all a matter of how to make information security usable. Balfanz et al. [24] composed a team of HCI and security researchers and presented five lessons on usable security. The first, usable security, starts from the ground up: “you can’t retrofit usable security”; Lacohee et al. agreed with this lesson and posited that “security must be implemented across the board at the beginning of a systems build/design process, it cannot be retro-fitted as a bolt on afterthought, it must be part of the end-to-end process” [41]. In addition, technological tools cannot replace security, as “tools aren’t the solution.” This can be seen in the study of Whitten and Tygar on the relationship between usability and information security, where they analyzed Pretty Good Privacy (PGP); they found many problems with the use of encrypting and digitally signing emails [29]. Third, security needs to be designed into all layers, not just the ground, and be suitable for users; thus, usable security should mind the upper layers.” The fourth lesson is to “keep your customers satisfied” by designing security for the average user and the fifth is “think locally, act locally” because there is not a universal solution for security problems. In 2007, Schultz [29] investigated usability in information security and found that there were not enough studies in the field and that researchers needed to focus on human factors in the information security tasks. A similar point was developed by Roth et al. [76] when they studied security and usability with particular attention to email. In their research, they developed an engineering design method towards non-intrusive secure mail with optimum security and usability by applying the three principles for designing protection mechanisms. Moreover, Weir et al. [21] explained that security procedures designs often excluded human factors and focused more on a technologically valid security system; however, those designs will be useless if intended users do not understand the procedures or find them too difficult. Thus, usable security is about finding the balance between security level, usage perspective and users [21].

2.4 *Assessment of Web-based Information Systems*

2.4.1 Web-based information systems

When assessing web-based information systems, many researchers proposed and/or evaluated methods for their usability. Oztekin [15] proposed a decision support system (DSS) for usability evaluation of web-based information systems that uses support vector machines, neural networks, decision trees and multiple linear regression. DSS reveals the interaction between usability and its factors in the domain of web-based information systems; the Usability of Web-based Information Systems (UWIS) checklist (mentioned later); developed by [14] is used in gathering the data. For example, one application of DSS in a university system revealed that using more optional control buttons in the system and clarifying them further is the most critical usability improvement strategy.

2.4.1.1 Assessing web-based information systems quality

Some authors also evaluated web-based IS quality. Some of the major assessment techniques were ServQual and WebQual. Oztekin[15] proposed webQual, a modified version of servQual, which was more applicable to web-based information systems, with six dimensions. In fact, ServQual, developed in 1988 by Parasuraman, Zeithhmal and Berry, is a questionnaire widely accepted for assessing service quality in any type of organization with 5-point distance semantic scale or a 7-point Likert scale. WebQual also used the 28-question checklist developed by Li et al. in 2002, which is widely accepted in the field [15]. The value added to webQual is that it assesses the user perception of the quality of web-based IS using quantitative metrics

[15]. These metrics are from qualitative customer assessments and can help managers in decision-making [15].

2.4.1.2 Usability and quality of web-based information systems

Fernandez and his colleagues attempted to summarize the usability methods that had been applied to web applications in the past fourteen years. They asserted that "Usability is considered to be one of the most important quality factors for Web applications, along with others such as reliability and security" [12]. The methodologies for assessing quality and usability of web-based IS often contains similar sets of items; therefore, Oztekin et al.[14] proposed UWIS, an extended form of servQual, which "measure the usability of web-based information systems including the dialogue principles for user interface design according to the standard ISO 9241-10 (ISO, 1996) and usability heuristics (Nielsen, 1994)." [14] ServQual dimensions are: quality of information, reliability, responsiveness, assurance, and integration of communication. UWIS dimensions include all the previously cited dimensions plus controllability and navigation. In addition to the 32 questions generated by these dimensions, UWIS measures effectiveness, efficiency and satisfaction; the last three are contained in the definition of usability according to ISO 9241-11, 1998. UWIS methodology has a major drawback because it assumes a linear relationship between the elements of the dimensions and the usability indexes.

2.4.2 Web-based services

2.4.2.1 Web-based services usability assessment

"The web services provided by web-based information systems (WIS) have gained increasing importance in contemporary society. The users of WIS would like to find information in a fast and convenient way. Yet, unfortunately, many WIS are still too slow to be usable and cannot satisfy many of their users" [15]. Some previous assessment methods for web-based services usability include:

- A generic test environment by Lindenberg and Neerincx in 1999 that measured the usability of web-based services as regard to measures of effectiveness, efficiency and satisfaction, which was later applied by Benbunan-Fich (2001) [43].
- The use of protocol analysis by Neerincx in 1999 to evaluate the usability of a commercial Web site [43].
- A recommendation from Frokjaer et al. (2000) on the three parameters of Lindberg and Meerincx, stating that these parameters should be treated as independent variables when testing for usability [43].

2.4.2.2 Web portal or web interface services use

When users get email accounts from providers, they are more likely to use other services providers' offers, such as reading their news, using their chat systems and, more important, seeing their ads, which is their main source of revenues. "Driving traffic to their sites and making users stay for longer periods are important for portal firms because Internet-based advertising is their main source of revenue." [63] In addition, the more providers have to offer, the more popular they get and more companies and merchants pay for their ads. Moreover, a more repeated use allows providers to capture the preferences and attributes of users, to improve their designs and services to better market themselves or to meet their customers' expectations [63]. Telang et al. investigated the drivers of web portal use by comparing three complementary measures of their use (frequency of use, length of visits and repeat use) to three categories of services offered by providers [63]. They asserted web portal services are categorized in three parts that are: search, information and personal services. Search services will allow a user to look up information; information services involve new, weather, sports and such; personal services are defined as applications that require a username and a password for access, for instance, as in emails [63]. The Telang et al. paper is interesting to our investigation because it shows that email accounts are services provided by the website as a personal service in order to attract users to other services. In addition the authors asserted that the gratuity of the service makes it appealing to a vast majority of people [63].

2.4.2.3 Important drivers of web services use

In the online services world, participation is voluntary; thus, satisfaction is a determinant of adoption and an increase in satisfaction would lead to loyalty (Weir et al. [20]). Competitors are just one click away (Telang et al. [63], Fassnatch et al. [56]); thus, quality is also perceived as very important in determining choice of user. In fact, new features that appeared regularly on web portals aimed to lock in users and increase repeated interactions as well as frequency and length of use [63]. Besides, brand loyalty induces repeat use because of uncertainty regarding others brands, but also it initiates a routine that diminishes the cost of thinking and, even more, there is more assurance in the quality for the price paid [63]. The findings of the study in [63] demonstrate that personal services are important drivers of loyalty and search services are the key drivers of portal traffic. Another valid point from this study is that if users register for personal services, they are likely to use the other two services. The authors also noted that dissatisfaction and demographic characteristics such as age, gender, race and wealth played some role in web portal use [63]. From this 2005 study, Yahoo and Excite came in first when it comes to strong loyal bases among the other portals [63]. The next section focuses on web-based services quality as it relates to customer satisfaction and how it is a predictor of their behavioral intentions.

2.4.2.4 Consequences of web-based services quality

Fassnacht et al. defined "web-based services as services delivered via information and communication technology where customers solely interact with a user interface on the World Wide Web (WWW) in order to retrieve desired benefits" [56]. The quality of web-based services was further defined "as the customer's evaluation of the degree to which a Web-based service is able to fulfill relevant needs effectively and efficiently" [56]. The services were of two forms: supporting services aid in the purchase of goods or "traditional services" and stand-alone services [56]. Stand-alone services are separated into pure service offers, which "enable customers to perform certain tasks over the WWW, for example, keeping a bank account or sending e-cards" and content offers, which "provide online access to various forms of content that customers can retrieve" [56]. Likewise, according to Udo et al., web services quality, also called e-services quality, represents the perception, judgment and evaluation provided by a virtual marketplace [38], and a good appreciation from the customer increases the frequency of use of the services and thus profitability for the company.

Overall, they found that the major consequences of web-based services quality were perceived value, customer satisfaction and customer loyalty [56]. Perceived value is "the customer's evaluation of the ratio of service performance received to the price paid"; customer satisfaction is "framed as the customer's overall response to the total purchase and consumption experience with a Web-based service over time" and customer loyalty “in the sense of brand loyalty, namely, as the customer’s intention to consistently use and recommend a web-based service in the future” [56]. Trust is “a customer’s favorable attitude towards a web-based service that her/his positive expectations regarding this service will be met in the future” and in addition the results showed that trust plays a major role in loyalty and, thus, indirectly affects quality.

2.5 Trust

2.5.1 Definition of trust

According to the Oxford English Dictionary, trust can be defined as: “the belief or willingness to believe that one can rely on the goodness, strength, ability of somebody or something” [46].

Trust has been characterized as a multidimensional construct [19], dynamic, evolving and multifaceted in nature [54]. Many researchers (Lacohee [41], Roy [54], and Wang [80]) recognized that the concept of trust is difficult to define and its meaning varies across multiple disciplines. As such, a social science definition of trust is “an attitude of positive expectation that one’s vulnerabilities will not exploited” [41]; a definition of trust in marketing is ‘‘a willingness to rely on an exchange partner in whom one has confidence’’ and in psychology trust is ‘‘an expectancy held by individuals or groups that the word, promise, verbal, or written statement of another can be relied on’’; in philosophy trust is the ‘‘accepted vulnerability to another’s possible but not expected ill will toward one’’ while in management trust refers to “an informal governance structure that enhances the effectiveness of transactions whether they take place in markets or within a hierarchy” [80]. From these definitions, a list of adjectives stands out: attitude, willingness, expectancy, vulnerability and governance. These qualifiers represent characteristics, concepts or determinants of trust.

2.5.2 Characteristics of trust

Many researchers [80, 54] used the four characteristics of trust defined by Mayer et al. in 1995 as a basis for their investigations. Moreover, Wang et al. [80] defined those characteristics for an online environment. Consequently, trustor and trustee are required in a trusting relationship. The user of the website is the trustor and the website represents the trustee, the party to be trusted. The relationship between the two is based on the degree of trust the user has in the website and the trustee’s ability to act in the best interest of the user. Then, vulnerability from the part of the two parties is necessary in a trust medium. Produced actions that Roy et al. [54] called expectations that are all based on some risks the trustor and trustee take and, last, subjective matter that the trustor cannot monitor nor control. In their study however, Fassnacht et al. [56] used two characteristics; the type of construct trust represents and the referent of trust or trustee. The type of construct refers to “a particular attitude towards the future” and the trustee represents the forms of trust. Structural trust (trust in a system or an institution) and interpersonal trust (trust in another party other than system or institution) were identified as the two forms of trust [56]. As an example, trust in a particular brand is an interpersonal trust and trust in the web as a medium is a structural trust [56].

2.5.3 Concepts and determinants of trust

Roy et al. [54] (2001) defined the four concepts composing trust as: integrity of the organization based on concepts such as confidentiality of information; benevolence, which is an aptitude to engage in mutually satisfying exchanges; ability of the sellers such as their characteristics and competencies; and propensity of the user, which is the general pre-disposition or desire of the individual. Wang et al. called three of those factors (integrity, ability and benevolence) antecedents to overall trust [80]. Flavian et al. in 2006 confirmed these four concepts without referring to them as concepts. For instance, they defined trust "as a group of beliefs held by a person derived from his or her perceptions about certain attributes" [19], which relates to the definition of propensity. Also, they enumerated the three dimensions of trust. One dimension is perceived competence in a website, which could be well assimilated to ability in Roy et al.; another dimension is benevolence and one final dimension is honesty, similar to integrity in [54.

While Kim et al. believe the determinants of trust are different based on the stages of the online transaction; Wang enumerates six dimensions for determinants of online trust. Those are information content, product, transaction, technology, institutional, and consumer-behavioral dimensions.

2.5.4 Models of trust

The literature on trust is mostly based on trust in commercial transaction and trust of website. As some e-commerce studies of trust are concerned about the disclosure of financial and personal information to online merchants, in a similar manner, when using a website, a user faces the problem of trust in storing personal emails and information on a provider website. Two models have been repeatedly used and are widely accepted for modeling online trust. The Model of Trust for Electronic Commerce (MoTEC) was developed by Egger in 2001 and it defined four factors that are likely to affect consumer trust: the pre-interactional filters taking place before any online interaction, the interface properties of the web site, the information content of the web site, and relationship management [80]. Another model in 1999 focused on the factors that communicate trustworthiness, the Cheskin/Sapient Report, which enumerated six building blocks of online trust that were seals of approval, brand, navigation, fulfillment, presentation, and technology [80]. A total of twenty-eight components can be regrouped to form the six building blocks or website interface cues that would foster perceived trustworthiness.

2.5.5 Enhancing the perception of trust

Wang et al. [80], among others, listed the ability to deliver a service as promised, the presence of privacy policy or statement on the website as some of the elements that enhance the perception of trust online. In fact, the importance of posted information, such as privacy statement or statement regarding how a user's information will be used, is a factor that affects the trust. Johnston et al. [46] posited that other than technical security features, e.g., the user's feeling of control of the interactive system also impacted trust. Customer confidence is impacted by user need, capacity and willingness as well as the seller (or here the provider) ability, benevolence and integrity [54]. The factors that build and foster trust are expertise, likeability and similarity to customers; in addition, customers evoked competency, benevolence and problem solving as indicators or trust [80].

2.5.6 Trust and web interface design

On a website, trust is important because the users do not really know where the central base with the data is located or who has access to the information they store. Lacohee et al. [41] states that a majority of users usually search for signifiers of trustworthiness on a website for their own security. As in commercial transactions [80], providers should convey their trustworthiness to their first-time visitors to transform them in customers. The interfaces through which they communicate with visitors are therefore really important. They should be usable and channel trust. Wang et al. [80] affirmed that the most effective way of enhancing trust is by applying trust-inducing features to the websites. Kubilus pursued this concept in saying that those features will be similar to the design features for effective interface usability [80]. Therefore, Wang et al. [80] proposed a framework for boosting user perception based on four dimensions, graphical design, structure design, content design and social-cue design. In addition to the four concepts of trust previously mentioned, on their quest on trust and interface usability, Roy et al. enumerated five concepts for interface usability, which included ease of navigation, consistency, learnability, perceptual limitation or perception and user guidance and support [54]. Their analysis revealed that all of these factors except from consistency are critical for a favorable user perception on trust, but all the factors are important for a trustworthy website design.

In email transactions, the recipient needs to trust that the provider will make proper use of the information in the email and that through the provider’s site no other person will have access to the information. The user’s perception of the website affects the likelihood of using it.

In 2006, Lacohee et al. undertook a study with controversial results. Conversely to general beliefs that secured websites enhance trust level, the authors demonstrated that the relationship is intertwined between trust, risk, privacy and control of information, responsibility and levels of confidence in relation to the likelihood of restitution being made if a loss is incurred [41]. Given the fact that most research tend to ignore the role of restitution or restoration after a compromise in information security, it was remarkable that Lacohee et al. [41] considered user's perception after facts as a factor of online trust.

2.5.7 Factors of trust in an online environment

Previous studies in computer security focused on the subject of trust on commercial websites. Trust is an abstract concept that cannot be measured or quantified. Among other principles of online trust defined by Hemphill, business policies on disclosure of personal information, options for how consumers' personal data could be used, permission for consumers to access and view their personal data are few of the principles applicable to online transactions [80]. Yet, Lacohee et al. [41] attested that many service providers and policymakers wrongly believe that proof of security on a website will attract a user. In addition, the authors advance that lengthy privacy statements confuse users rather than clarify information about security of a website. Rather, the authors in [41] argued that users focus on what will happen when something goes wrong. Their study backed up their arguments when users' perceptions showed that users are aware that there is no 100% security and that they were more trustful if a website stated their risks and ways they could regain their loss if a loss occurs. As such, three elements that engender online trust are: confidence that restitution could be made by a third party, assurances about what could or could not be guaranteed and the presence of fallback procedures if something goes wrong [41].

2.5.8 How the perception of trust affects the loyalty to the website

As Lacohee et al. studied the advantages that the user gains from using a web service helps them evaluate whether it is worth the risk to use the website [41]. Flavian et al. [19] analyzed the influence of perceived website usability on user trust and satisfaction and the incidence of usability, trust and satisfaction on the loyalty of these Internet users. Fassnacht et al. [56] demonstrated that trust is a major influencing factor of loyalty. They also affirmed that customer satisfaction has a large positive effect on trust [56]; thus, trust indirectly affects loyalty. Users make their opinion of online sites based on communication with peers and trusted third parties and the affect of the mass media [41]. Similarly, at the prior exploratory stage, Flavian et al. believe that reputation, propensity and testimonials perceived by users affect their trust; then, at the commitment stage, experience and knowledge accumulation influence trust [19].

Flavian et al.'s [19] results revealed a positive parallel relation between the degree of website loyalty and degree of trust, the perceived website usability and degree of satisfaction, the website user satisfaction and the degree of trust, the website consumer trust and consumer loyalty, as well as consumer satisfaction and degree of loyalty. Moreover, usability was not found directly connected to website loyalty; instead, usability effects were dependent on consumer trust and satisfaction.

2.5.9 User perception on trust, attacks and the privacy of their personal information

Lacohee et al. additionally found that reputation based on brand and prior experience and recommendation from trusted third parties, played a major role in users' decisions for online services, and users also tend to stick with those trusted companies they have experience with in the physical world [41]. Interestingly, this is the exact principle on which attackers base their phishing attacks. Sometimes the amount of information required by websites goes above the users' perceptions of what it needed. For example, some reported giving false information when they feel their privacy is invaded [41].

The singularity of the findings in the Lacohee et al. [41] study opposed to many of the other studies in the online transaction or services domain and the attempt of Udo et al. [38] to analyze risk perception, lead to our investigation of risk perception in information security and specifically email accounts. Trust, usability, satisfaction, loyalty, security, user perception as a factor of all these previous items were all extensively researched and appear in the literature. However, very few studies accounted for risk perception by the user in information security and in our case email accounts. Lacohee et al. showed that risk perception affects online trust [41] and Udo et al. examined the effects of risk perception on satisfaction and behavioral intentions in e-services.

2.6 Secure Communication

The importance of secure communication has increased due to the large exchange of information online, the use of the Internet and the rise of cyber criminality.

Confidentiality, availability, integrity and non-repudiation constitute the main requirements for secure communication [58]. Non-repudiation relates more to commercial transaction or transaction with contracts; integrity refers to the safe delivery without external modification; availability assumes that the information to transmit cannot be hidden; and confidentiality refers to the protection from unauthorized disclosure. To control the access to information, many authors have suggested the use of authentication. Authentication in secure communication “refers to a process of ensuring that subjects are really the subjects they claim to be” [58]. With authentication, integrity, confidentiality and non-repudiation will be checked [58].

2.6.1 Authentication methods

Other secure authentication methods other than passwords exist, but few systems utilize them because of their lack of usability [29]. Precisely, Roth [76] argued that numerous supports for strong email security exists, however, many users do not take advantage of them because the costs associated with the use of this security systems is too high, not monetary cost but cognitive efforts and steps, as well [76]. While security is added in the two-factor authentication method, it would have been remarkable if the Gunson et al. [60] study compared the usability of the two-factor authentication over the one factor authentication.

Keith et al. evaluated the usability of passphrases for authentication; passphrases are different from passwords because they contain multiple words [55]. Passphrases are more memorable because they form a sentence; in addition, the length of the string exponentially augments “the time required (guessing) in using brute-force attack methods" [55]. The authors argue a passphrase length of fifteen to twenty-five letters significantly improves password strength even if it is made of only lower case letters [55]. Yet Vu et al. [29] required creating sentences with embedded digit and character to achieve a crack-resistant password. On the one hand, the increase in security of passphrases is not recognized by the Vu et al. study, but on the other hand, embedding digit and character might re-create the memorability issue even if it increases the security. This goes back to the tradeoff between usability and security.

In electronic email services, password-based authentication methods are prevalent. Passwords need to be usable and secure.

2.6.2 Password usability

Extensively large literatures on a particular set of single-factor authentication methods (passwords) exposed that a secure single-factor authentication method is very difficult to remember; thus, users expose their password by writing it down or using the same password on many applications ([21], [60]. There are many authentication methods, but passwords are mostly prevalent [21].

Secure passwords often pose the problem of memorability ([21], [60], and [20]). Frustration and delay are often consequences of forgotten passwords [21]. The number of passwords a typical Internet user possesses and has to recall increases with every service registration. Gunson et al. noted that an individual can only memorize four or five regularly used passwords and in the workplace, that number goes up to sixteen [60]. Various policies and requirements exist on many websites to improve the security of passwords.

Pin and text passwords are examples of knowledge-based authentication methods that users are accustomed to despite their low security level. Some other knowledge-based passwords are graphical passwords that have been increasingly used in recent years [60]; however, their usability has not been sufficiently studied [60]. Nevertheless, a graphical password can be easily hacked by an attacker who is familiar with the user. Social engineering methods, such as phishing, spoofed interfaces and keystroke capture software, are predominantly used by attackers for collecting passwords [61]. It becomes extremely important to find the appropriate balance between users' perceptions of convenience and security.

2.6.3 Password and security questions

A general form of authentication used in many online systems and specifically in email services are password and security questions. Passwords could be made up of text, numbers and non-letters: "the Federal Information Processing Standard (FIPS) (1985) on password usage is one of the earliest set of guidelines for creating strong passwords; it states that passwords should be approximately five to eight characters long and be composed from a 95-character set including uppercase letters, lowercase letters, numbers, and other non-letters" [55]. The previous literature explained largely that passwords were insufficient for security because they are guessable, they could be forgotten if too complex, they can be divulgated by writing them down or using the same password across multiple domains ([29], [21], [60], [55]). Some interfaces such as banking online services adds security questions to users' passwords as a second layer of security; Keith et al. [55] called this a set of multiple inputs. Other information systems, such as computer logins or web-based mail services, however, utilize security questions as an alternative to passwords. The user is asked to choose, give or compose their security questions and to provide their answers, which is stored for future verification. Keith et al. posited that those were easy to guess, first, by someone who knew the password creator well and, second, in the case where the security answer is made up of only one word and could be retrieved using dictionary and wordlist attacks [55]. Many authors suggested more research studies in the field of information security that would include the users of the system and the human factor ([29], [58], [20], [13] and [55]).

2.7 User perception

A definition of usability engineering is given in [20] as "a process by which systems are built and tested with empirical methods to achieve efficiency, effectiveness and satisfaction for specified users performing specific goals in a particular environment." Usable systems need to be designed to minimize user errors. Other types of errors in HCI except goals errors, that [65] focused on, are plan, action and perception errors. This section focuses on the perception of users on authentication methods, how brand credibility affects customer's loyalty, the customers' appreciation of e-service quality, satisfaction and intention and why users switch their email services.

2.7.1 Perception of user on authentication methods

2.7.1.1 Comparison of authentication methods

We reviewed three literatures in authentication methods in the banking industry. Even though email services are different from banking services, we believe the user perception on authentication in the banking domain could give us some insights on user perception towards authentication methods. Gunson et al. [60] investigated user perceptions of security and usability of single- and two-factor authentication in automated telephone banking. This study is recent (2011) and of interest because it deals with authentication factor. Even though it is not in the online services or web services domains, it gives us a perception of users' beliefs toward authentication processes. The authors defined three categories of authentication methods: what you know, what you have, and what you are; those three components relate respectively to information only known to the user, and a possession indicated for the use of the individual only and some physical attributes of the user [60]. Thus, single-factor authentication involves only one of those components while two-factor authentication uses any two-combinations of the components [60]. The advantage of the latter is that it offers an additional layer of security over a single-factor authentication. The authors analyzed the usability of the two methods in automated telephone banking using real life customers. They employed a Likert-type questionnaire to measure the perception of the security of the system, the appreciation users had of the amount of information they were required to input, the cognitive issues, the fluency and transparency of the system, the system performance and issues regarding the voice of the service. Overall, the usability, convenience and ease of use of the single-factor system were rated significantly higher than the two-factor system; in addition, the two-factor system took longer time. However, participants valued the security offered in the two-factor authentication method [60].

These findings confirmed the importance of usable security, which aims to find an optimal trade-off between usability and security. It also emphasizes that secure authentication methods are perceived as not easy to use. Complex mechanisms are deemed secure; however, they seemed too complicated for the average user. This can be seen when Weir et al. [20] examined three two-factor methods of e-banking authentication using regular customers of the bank. All three methods were perceived equal in security level in general but individual participants favored the method they perceived the least secure because it was easy and convenient [20]. Even when the study was repeated, the majority of the participants preferred the fast and easiest two-factor authentication method; the authors suggested that user choices could be based on "a variety of effects including selection bias, cognitive dissonance and practice effects" [20]. In another study performed later in 2010 with another group, Weir et al. [21] named the three authentication methods knowledge-based, object-based and biometric-based as examples of passwords, bank card and fingerprint, respectively.

Using the banking system again, the authors [21] investigated user preferences in authentication methods using a two-layer password (1-factor) method and two alternative two-factor authentication methods; and discovered the following:

- Users preferred the personal nature of passwords and were reluctant to using new methods of authentication
- Users favored convenience over usability or security in authentication methods
- Knowledge-based authentication methods were seen by many as portable and more convenient.

In short, convenience, personal ownership and habitual experiences of processes were the main indicators of preference [21]. The results lead the authors to believe that users were not aware of the security threat of a password on the Internet and more media coverage and education is needed in the area [21]. Also, they argued that doubt or lack of understanding of unfamiliar authentication methods might be the source of user rejection of new authentication methods [21].

2.7.1.2 Passphrases as authentication method

Another authentication method suggested by Keith et al. [55] is the use of passphrases. Since previous studies proved that users geared more towards knowledge-based authentication, this study is appealing in terms of alternative methods to two-factor methods (high security but difficult to use) and passwords (easy to use but low security). In fact, the authors argued that effectiveness and efficiency in security could be achieved using passphrases [55]; thus, they conducted a study to assess the usability of passphrases. The effectiveness was based on the strength of the password against attacks, the usability illustrates the ease to remember and the capacity to login and also the satisfaction was analyzed as the perception of the user of effectiveness and usability. After all, the usability of passphrases could not be verified even though they were perceived as more secure than passwords and equally as memorable. The users made several unsuccessful login attempts [55] and the frustration is still present, similarly to when passwords recall remained difficult.

2.7.2 Customers' appreciation of e-service quality, satisfaction and intention

Udo et al. [38] surveyed 211 senior business administration undergraduate students in a large public university with at least one online shopping experience, six months prior to the study using a seven-point Likert-scale. They were interested in evaluating the effects of risk perception on customer satisfaction as well as customer continued use of the service and their perception of service quality [38]. The authors proposed a study model and formulated some hypothesis for interactions between satisfaction, behavioral intentions, PC skills, perceived risk, service convenience, website content and website quality [38]. PC skill primarily impacted service convenience and quality secondarily; website contents had a positive impact on perceived services quality and the latter strongly influenced behavioral intentions which in turn drove satisfaction [38]. Unfortunately, the risk perception effect on customers' satisfaction and intention could not be determined; yet, less perceived risk positively affected the perception of web service quality [38].

2.7.3 Brand credibility, satisfaction and customer's loyalty

In 2008, Sweeny and Swait undertook a study of the effects of brand credibility on customer loyalty [47]. Satisfaction is a positive emotion of the user that affects loyalty; in fact, Weir et al. stated that "satisfaction is theorized to be determinant of future adoption" [20]. Equally, brand credibility is a perception of users that can affect their loyalty. Brand credibility is "the belief that the brand is capable and willing to act on its promises" and was measured based on expertise and trustworthiness [47]. In their model of study, the authors [47] considered that satisfaction, loyalty commitment and continuation commitment were all antecedents of brand credibility, whereas word of mouth or recommendation and switching propensity were all affected by brand credibility. Moreover, they assumed a reciprocal relationship between loyalty commitment and continuance commitment and that satisfaction impacts loyalty commitment unilaterally. Loyalty commitment indicates "the underlying affective notion of commitment, including the desire to maintain a relationship in the future"; and continuance commitment "reflects the need to maintain the relationship considering the perceived switching costs" [47]. Those assumptions were tested, but the results demonstrated that brand credibility directly affects customer satisfaction and through satisfaction there is customer loyalty. Recommendations resulted from satisfaction, a cumulative experience-based evaluation. In addition, loyalty commitment reduced switching propensity [47].

2.7.4 Perception of user on email service switching

Previous researches as seen above showed a positive direct relationship between satisfaction and loyalty. Additionally, loyalty reduced switching behavior [47]; however, many web services providers lose their customers to other competitors. Particularly, many individuals replace free personal services such as email. Kim et al. [37] investigated the reasons of the switching behavior and found that perceived customer satisfaction with the email service, the availability of attractive alternatives and switching cost explained the dynamics of switching. Providing email accounts is a service rendered to potential clients [37]; thus, providers deploy a huge effort in maintaining their customers.

Customer satisfaction with email service was measured based on design, stability, spam blocking and storage capacity [37]. Switching costs were appraised based on setup cost (time and effort invested to register for a new email account, configure new settings,) and continuity cost (archive and import existing emails, distributing new account information and the risk of losing existing contacts) [37]. The authors assumed that the attractiveness of alternative email services was based on users' perceptions, which were influenced by advertisement, word of mouth, media and rumor [37]. Based on previous literature, the research model estimated the relationship between satisfaction and intention to switch to be moderated by the switching costs and the availability of attractive alternatives. In addition, switching costs and the availability of attractive alternatives directly impacted the intention to switch email services [37].

A survey instrument of 27 questions was created using a seven-point Likert-type scale; most questions were taken from existing studies but the authors constructed the storage capacity and spam-blocking questions [37]. The authors chose to get their participants from a proprietary list of an online marketing research company and obtained 1,408 valid responses [37]. The findings verified all the authors' assumptions except from the moderating effects of switching costs on the relationship between customer satisfaction and intention to switch email services [37]. It is yet to be known whether the intention to switch actually developed into switching [37]. In sum, customer satisfaction or dissatisfaction and attractiveness of alternatives determine email- switching behaviors.

Kim et al. [37], based on literature, enumerated the dimensions of satisfaction in online services as

1. information quality (e.g., consistency, accuracy, timeliness, and ease of understanding),
2. quality of user interface (e.g., feedback mechanism, learning effect, and system performance),
3. perceived usefulness and ease of use, and
4. perceived quality of on-line stores (e.g., price competitiveness, brand, security, product differentiation, and product quality)

Surprisingly, these dimensions of measuring satisfaction do not include information security. This again points out the lack of sufficient literature on user perception and security.

2.8 Summary

All the reviews of literature on online experience, customer satisfaction, human perception and human error point out some great criteria for analysis of web-based information systems.

However, very few focused on the security as being an important part of analysis. Few mentioned policies or privacy statements for making the user feel secure.

Further, none of them expanded on the security of email services as when confronted with an attacker. A great deal of literature investigated attacks on information systems, on the one hand, and, on the other hand, on satisfaction, user perception of web-based information systems. Our study is different than all of the other studies because it combines the findings of each of these domains to assess email services accounts from the security point of view. It is important to know how well protected the free email accounts offered to any individual are and also how the use of the Internet leading to globalization and generalization of information constitute a potential for attacks on email accounts. We will investigate the security of email accounts by measuring the risk associated with their use.

Most if not all of the findings of our literature review of related topics were based on survey questionnaires. Moreover, most of these studies used the Likert scale type of questionnaire for the survey. Gunson et al. noted the advantages of this method as being more effective in measuring change over time, having a high degree of validity and reliability and being “more natural to complete because it maintains [survey participants’] direct involvement in the process” [60]. In our methodology, we use a new and widely accepted assessment method applied to information security. This methodology is more appropriate to our analysis because it is based in the domain of information security and it is an elaborated survey preparation and conduction process to assess the security risk in a system.

Chapter 3: Email Accounts and Risk Classification

3.1 Email Accounts

3.1.1 Email Account Domains

There are many websites offering email accounts nowadays. In general, users in the United States have accounts on .com domains such as Gmail, Yahoo, AOL, and Live. The focus in this research is on the US population because people from different cultures or countries are accustomed to different websites. In fact, individuals in French speaking countries are more accustomed to the .fr domain and people in Canada are familiar to the .ca domain. There exist a huge number of online providers who allow the creation of email address in their domain with receiving and outgoing messages free of cost. We recorded Gmail, Zohomail, Icloudmail, AOL Mail, Windows Live Hotmail, GMX Mail, Yahoo Mail, Fastmail, Shortmail, Bigstring, Gawab, Inbox, Mail, Lavabit, Lycos Mail, Zapak, Hotpop, Mywaymail, Care2mail, Myspacemail, Facebook Mail, Mozilla Thunderbit, Netaddress, Walla, and Excite.

3.1.2 Previous Studies on Security Perception of Email Providers

There are many sites that rank different email providers. Specifically, in June 2012, a free email service comparison review in Top Ten Reviews [10] classified the top ten email providers according to their security levels and the rating from the highest to the lowest was as follow: Gmail, AOL, Yahoo, Inbox, Fastmail, Windows live, Mail, Lycos mail, Care2 and Goowy. The security parameters were defined as "the features the free email service provides to keep your email safe from viruses, spam and phishing.”[10] All of those accounts except Lycos and Goowy scanned all incoming and outgoing mail for potential dangerous threats, virus or worms and used a phishing filter. All those providers with the exception of Lycos had a restriction on automatic attachment download and a spam filter system. The top six had a secure signing system for password protection (https encryption). In October 2012 according to their security level, Gmail, Windows live and Yahoo had the same security level of 10; AOL was behind with a score of 8.13 out of 10. The security parameters under consideration at that moment were secure sign in, spam filter, report, virus scanning, phishing filter, image blocking and restricts automatic download.

‘Secure sign in’ refers to password protection using https encryption. ‘Spam filter’ denotes whether known spammers or suspicious emails are blocked or filtered into the spam/junk folder by the email provider with the option to adjust the strength of the filter. ‘Report spam’ as it is worded refers to the ability to notify the email provider of a spam. ‘Virus scanning’ checks whether incoming and outgoing emails are scanned by the email provider for potentially dangerous threats like viruses, worms or Trojans; similarly the feature ‘restricts automatic download’ refers to whether the email service verifies if the attachments received do not contain those dangerous threats. In addition, ‘image blocking’ checks whether the email service blocked infected emailed images and the feature ‘phishing filter’ verifies whether the email service blocks malicious emails that request personal information, like passwords and credit card numbers, or warns users of potential threats. This analysis was very insightful and contributed to the establishment of the attributes and characteristics in our study. However, our study takes this ranking further by incorporating the elements of the account creation process and other features that the authors in [10] cited for consideration on the overall ratings of the email service but were not included in the security ratings. The authors believed that features such as chat system or email account storage capacity are related to the security of the email account.

3.1.3 Email Accounts under Study

We did not take into account providers that require additional subscription with the free email account. For example icloudmail is specific to apple users, the application requires an apple ID; Facebook email is exclusive to Facebook subscribers only; this also applies to myspacemail. In addition, this analysis did not include business email such as Microsoft Outlook which can be purchased with Microsoft Office and commonly used in enterprises and Zoho mail called a business email provider with multiple users, up to three, for the same account.

A first selection process led to the disqualification of some providers. Fastmail offers email services for business, individual or multiple users and was disqualified. Shortmail imposes a limit on the number of characters in an email thus was disqualified. Lavabit mail offers different kinds of account for users some of them with a fee and was disqualified. Bigstring is a private wall with email access and was disqualified. Inbox and Netaddress are not completely free and were removed from the analysis. To our knowledge, Gawab, Zapak, Hotpop mail systems no longer exist. Mozilla Thunderbit is an application which needs to be downloaded before its usages therefore it was removed from the analysis. Walla is in Hebrew thus disqualified. In a second selection process, Mywaymail and care2mail were disqualified because they start with a page creation then an email service. Excite is a toolbar installation process and requires answering their sponsor survey questions before accessing email services; therefore was disqualified.

Thus the email accounts under consideration have only one user, were provided online at no-cost and did not require subscription to any other services or belonging to any club or group. Users are capable of opening as many accounts as they like across all providers as long as any two on the same domain do not have similar username.

3.2 Risk Analysis Method

There are many works on risk assessment in information security. Bones et al. summarized the steps of risk analysis as the identification of the threats or possible damages to systems, an analysis of the impacts and likelihood of the threats and the evaluation of risk based on acceptance criteria [34].

3.2.1 Identification of Threats

The list of criteria used in the study was based on the previous elements noted in the literature for secure communication, email service switching, password usability and authentication, interface usability as well as the previously mentioned study [10]. The authors do not consider features such as IMAP and POP or setting files permissions because we believe the average user does not know or comprehend their utility. We defined two stages where the security of an email account is at risk. The setup stage is the initial moment where a user decides to create an account and register on a website. The usage stage is the period after setup where the user actually utilizes the account for his/her needs which could be to send and receive emails. In addition, the setup stage consists of three sub-categories: the steps for account creation, password sophistication and security questions. The usage stage takes into account the filtering systems available, whether incoming and outgoing emails were scanned for threats, the storage capacity, and the availability of blocking features; but also the chat system, the attachments option and the password encryption.

3.2.2 Assumption for Data Analysis

3.2.2.1 Setup Stage

Steps for account creation were analyzed based on the number of interfaces or web pages users had to go through in order to finish their registration; it is implied that users will input information on each of the pages. Next, substantial analysis exists in the literature on password security. In an attempt not to repeat theses studies, the dimensions we chose to consider are email accounts requirements on password strength based on the password length and composition. Furthermore the composition was discussed in a sense of all the possible combinations of letters, numbers or characters (non-letters and not numbers). We did not take into effect the distinction between upper case and lower case letters because we did not want to put too much emphasis on the password versus the other attributes of security. Finally security questions were analyzed based on their number, their form and their quality. Table 3.1 below provides greater details on the elements of the analysis pertaining to the setup stage.

3.2.2.2 Usage Stage

Email accounts usually contain an automatic filtering system as well as filtering choices for the user. Their presence or absence will impact security. Spam folder specifically contains potential junk emails sent to the user. In addition, having the option of blocking certain email addresses was considered beneficial to the user security. The availability of other features such as chat system or mobile app was believed to have an impact on the security level. Whether attachments received on the users email account were automatically analyzed for virus or threat was another attribute of security. Finally password encryption varies on different providers account. Table 3.1 provides greater details on the elements of the analysis pertaining to the usage stage.

Table 3.1 Elements of Setup Stage and Usage Stage

Stages	Attributes	Characteristics
Setup stage	Steps for account creation	One interface
		Multiple interfaces
	Password sophistication	Length
		Strength
	Security questions	How many questions options
		How good are the options
		How many options required
		Type of requirement
		Minimum requirement for security question answer
		Display security questions & answers after sign up is complete
		Number of requirement for recovery
		Type of requirement for recovery
Usage stage	Spam blocking	Automatic spam filtering
		Spam reporting
	Email address blocking	Presence or absence of feature
	Incoming emails filtering	Presence or absence of feature
	Email account storage capacity	Unlimited
		10,303 MB
	Chat system	Presence or absence of feature
	Mobile app	Presence or absence of feature
	Connected to other apps	Presence or absence of feature
	Password encryption	HTTPS

	Scan incoming and outgoing mails for threats	Presence or absence of feature
	Attachments view options	Automatic analysis
		No analysis

We based our ranking on any features which could be actually observed and not on our perception. We use the minimum required information pertaining to all those variables to perform our analysis; this process will be what any typical user will go through. In fact, experienced users might protect themselves better for example by choosing “harder” security questions over “easy” questions used across many domains. We proceeded to create an email account on the five domains Yahoo, AOL, Gmail, MSN and GMX.

3.3 Risk Classification

We assessed the steps for account creation with five providers on the web. It is important to note that the steps for account creation change with time as technology evolves and providers incorporate new research findings to improve their security, usability and user perception. Even during our study, some requirements have been modified; for example hotmail evolved from a minimum of six characters for password to eight. Therefore, the application processes described below were based on the procedures at the time of our assessment and might not be conformed to the procedure to date.

In addition this also means that based on the number of years the email account has been in operation, the user’s password might not meet all the additional requirements of new accounts since users are not constrained to update their password to meet new security designs. For instance a password used to create an account ten years ago, if not updated, might not have the same characteristics as one created one year ago. Similar advanced changes are also observed at the usage stage, where more features are added or improved.

3.3.1 Yahoo Email Account

The Yahoo registration is a one page long application only. When signing up for a Yahoo account, a user is required to input their name, gender, birthday, country, language and postal code; then select an available Yahoo id and email. The user has the choice among yahoo.com, ymail.com and rocketmail.com. The password needs to be between six and thirty two characters and is case sensitive; cannot be your name or yahoo ID. The password strength blocks indicate whether your input is “weak”, “strong” or “very strong”. Any two-combination of characters is rated as strong and any three-combination is rated very strong; for example qwertY and qwerty65#. There is a hint telling the user that “For a more secure password, use both letters and numbers. Add special characters such as @, ?, % Mix capital and lower case letters.” [11] Yahoo indicates to users the security level of their password, but do not require any level. So our consideration for the analysis is their weakest level; in fact we verify that is was possible to create an account with six lower case letters as a password, specifically qwerty.

The account creation continues with two security questions and answers, a code that needs to be input, a final statement and the create account button. The final statement is “By clicking the ‘Create My Account’ button below, I certify that I have read and agree to the Yahoo! Terms of Service, Yahoo! Privacy Policy and Communications Terms of Service, and to receive account related communications from Yahoo!

electronically. To deliver product features, relevant advertising and abuse protection, Yahoo!'s automated systems scan and analyze all email, IM and other communications content." [11] The user could select a secret question from the list (what is the first name of your favorite uncle? or who is your favorite author?) or type in their question. The user has the option to add an alternative email address. There are nine security questions to choose from and an additional option to add your own question, so in total 10 options available for the first question. The second question has eighteen different preset questions and the option to type your own, so in total 19 options. The answers to the security questions must be a minimum of four characters long, not case sensitive. For the first security question "where did you meet your spouse" or "where did you spend your honeymoon" are questions with high security risks however, it suggested that the user was married. So we considered the other questions and they required knowledge of the specific information. For the second question the same analysis was made in regard to "who is your favorite author or "what is the name of your favorite sports team" and the options fall into knowledge of specific information. However, the analysis considered only the first list of questions because there are fewer. A list of all the questions for Yahoo sign up is provided is appendix B. After sign up is complete a screen displays your username, security questions and answers with an option for the user to print.

Yahoo stated that they scan and analyze all emails, IM and other communications content. In addition Yahoo provides a guide to security online on another web page. Yahoo has a filtering system for incoming messages and also an option to block up to 500 addresses. Spamguard is an automatic way of categorizing junk emails; however the user can classify other emails as spam and add them to the spam folder. Yahoo offers additional free apps provided by other companies such as Slice, YouSendIt, OtherInbox, etc and unlimited storage space. Yahoo also has a messenger system that can be used from your email account and the history of your chats could be kept within the account. There is a Yahoo! Mail app available for users. “Yahoo! uses SSL (Secure Socket Layer) encryption when transmitting certain kinds of information, such as financial services information or payment information.” [11] The account recovery process in Yahoo consists of answers to two security questions and the username of the account.

3.3.2 AOL Email Account

On AOL, you are required to input first and last name, choose your username based on availability and then input your password. The website helps you check the strength of your password, required 6 to 16 characters case sensitive; while giving you a hint “Strong passwords include special characters (!@.#). Avoid common words and names” As long as the number of characters is respected; the strength of the password used depends on the user. For example, the “password strength” case will indicate whether your password “could be stronger”, is “strong” or “brilliant”. However, it will not prohibit the use of a not strong enough password. But if the user inputs a common word such as qwerty or 123456, the system will not accept it and display “Oops! That's a little too easy to guess. Try something harder!” Once you click “Next”, you passed that page; a new page requires your date of birth, gender and zip code as well as a security question and answer which could be used for retrieval of your password. There is an explanation to why you are required to answer the personal questions: “You need to provide your date of birth in order to verify your identity in account management, and to ensure that you are eligible to use our products. Other data, such as zip code and gender are used to personalize your AOL experience (e.g., display local weather and news).The use of this information is governed by the Privacy Policy.” [2] The thirteen security question choices include popular question such as “what is your mother’s maiden name?” or “in what city were you born?” as well as not so common questions “what is your frequent flyer number?” or “In which city did your parents meet?” For our analysis, we assume the worst possible case, thus these questions were rated as general knowledge. A list of all the questions for AOL sign up is provided is appendix B. There is also an option to use your mobile phone number for added security. Another page appears where the user is required to type in the code shown in the image and “sign up” after reading the closing statement: “By clicking "Sign Up" below, you electronically agree to our Terms of Service and Privacy Policy (the "Terms"); you acknowledge receipt of our Terms, and you agree to receive notices and disclosures from us electronically, including any updates of these Terms.” [2] There is also a possibility of hitting the “Back” link to change any previous information and “Next” to continue. After sign up is complete a screen displays your username, security questions and their answers with an option for the user to print.

AOL has an instant messaging system which allows access from your email account’s inbox. AOL has an automatic spam filtering system and allows the user to create additional filters for incoming emails. AOL mail has an app and unlimited storage. In addition, AOL has a spam reporting system and allows blocking specific email addresses. All attachments are automatically analyzed for security threats. AOL mail blog educate users on security online and phishing. It is important to note that if another user clicked the link in [1], AOL interface for signing up is one interface and alternatives for security questions are mobile phone number or alternative email address; all the other steps remain unchanged. AOL recovery includes the answer to your security question plus your (first and last name) or (date of birth, zip code). Assuming that first and last name are easier to guess, this option was utilized in the analysis. The account recovery process in AOL consists of answers to the security question and a personal data question; and providing the username of the account. To our knowledge, AOL email accounts do not offer connection to other apps.

3.3.3 Google Email Account

Creating an account in Gmail is a one page application. The user is asked to input their first and last name and their username. The password needs to contain at least eight characters and a password strength check pops up to tell the user whether their input is weak or strong. The strength depends on the mixing of lower, upper cases, symbols or numbers. A message displays "Don't use a password from another site, or something too obvious like your pet's name." for instance the password qwertyui or qwerty12 is rated weak, not accepted; and 12345678* rated fair [6]. The strength could be too short, weak, fair, good or strong. A password is accepted when the strength is fair or above; all lower case passwords of length eight are accepted. Then the user inputs the date of birth, the gender, a proof of non-automated application, a location and clicks to agree with terms of services and privacy policy. At the next screen, your account will be created. Google stresses the addition of mobile number or alternate email address for password recovery. The user chooses to opt-in for two step verification; 2-step verification "adds a layer of security to your Google Account by requiring access to your phone - as well as your username and password - when you sign in. If someone steals or guesses your password, that person can't sign in to your account because they don't have your phone." [6] The optional security question list contains five preset questions with an option to "write my own question", thus a total of six options. No requirement exists for the answer. "What is your vehicle registration number or what was your first phone number" lead the authors to rate the question as requiring the knowledge of information.

Attachments to email are automatically analyzed. Google has a webpage dedicated to additional security information for a gmail account and two additional for phishing and malware. There is a Google app available in addition to spam protection and email filtering; however Google does not possess a specific address blocking feature. Gmail also has a chat system embedded in your email account and uses https settings by default. Google defined https (Hypertext Transfer Protocol Secure) as "a secure protocol that provides authenticated and encrypted communication." [6] The storage limit for a gmail account is 10,303 MB. Google mail is connected to other apps such as Green Robot, Auto-advance, Background Send, etc.

Since they are no security questions, in the event a user does not remember their password, gmail demands their username, an alternative email and the last password the user remembers in addition the "approximate" answer to the following questions: "When was the last time you were able to sign in to your Google Account? When did you create your Google Account?"[6] Based on the responses, the user could reset their password. It makes it very simple to enter any Google account provided that the user did not set the additional layers of security; in fact inputting “educated guess” such as a random password, the previous day for access and previous year for account creation were successful. Thus we did not count five requirements for account recovery but two.

3.3.4 Windows Email Account

On Windows live, a user can create an account on hotmail.com or live.com. After entering the desired id, the user inputs the password, which is a minimum of eight characters, twice. A help window displays the following message “Passwords must have at least 8 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, and symbols.” [8] This will be all the advice on password with no password strength check as on the other domains.

Hotmail has a one page application process. Hotmail has three options for password recovery, the user is obligated to choose any two; there are a mobile number, an alternative email address or a security question. The security questions are six and the answer must be at least five characters. Not case sensitive. This is the only provider in the analysis with a requirement of five characters for security answer. The users have only 6 choices of security questions to select from: mother’s birthplace, best childhood friend, name of first pet, favorite teacher, favorite historical person, grandfather’s occupation. These questions are very easy to answer even if the attacker knew the victim briefly [37]. After reading the final statement “Clicking I accept means that you agree to the Microsoft service agreement and privacy statement.” [8] The account is created. This is a one page creation process.

Hotmail has a junk folder for automatic analysis and also a messenger system. There is also a sweep module for categorizing emails and an option to block specific email addresses. Users of hotmail could also choose to block attachments from unknown senders who are not on their safe senders list; or send any incoming email from unknown user to the junk folder with the "exclusive" junk filtering option. As with other sites, users could also report junk messages which escaped the filtering system. "When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol." [8] There is an app for hotmail and unlimited storage since 2009. The user can connect to additional apps. Hotmail uses https for secure connection by default.

Even though the application process required two forms of account verification, in the event of a password loss; Hotmail performs only one form of verification and the user can reset their password.

3.3.5 GMX Email Account

Setting up your account on gmx.com starts with some information about your demographics (gender, first and last name, date of birth) and your location (country). You proceed to choose your username based on availability on gmx.com or gmx.us. The password security tips appear in a little box when you begin your password selection process and are a minimum of eight characters, mix of letters and numbers, mix of upper case and lower case letters and use special characters (e.g., @). The satisfaction of any one of those tips validates your password. No other security check notifies the security of the password you have chosen. An all lower cases password of length eight is accepted. Then the registration form requires an alternative email and a security question/answer in case you forget your password. Your security question must be chosen from a list of preset questions such as what city were you born in or what is your mother maiden name; there were nine security questions. It is important to note that all the questions in the list are general information on yourself and what you possess which any close relative or friends could easily know. There is no requirement for the security answer. The alternative email is not indispensable to your registration. Then there is a test to ensure that a human is using the program and the "I accept. Create my account" finish your registration process and confirm that you agree with the terms and conditions.

Once your account is created, you notice a spam folder which indicates that your account has an automatic filtering system. Your account can access up to 2 GB storage space for all file types: text, photos, music, videos, etc; your data reside on servers in a high-powered computer center and are extremely well protected from loss or theft. The provider also exhibits additional features namely SSL secure connection and configuration of your guest access.

Not too common is the presence of a files manager option which gives you possibility and access to a shared folder. Also you can manage your calendar through the organizer tab, participate in online forum from your email account. Your account comes initially protected with GMX spam protection which you could deactivate and reactivate at your convenience. Users could also report spams that made it to their inboxes. There is also a very basic filtering a black and white list where you can write addresses you do not want to receive email from. The last feature on the spam tab, allows you to clear the text pattern profiler; a guide would warn you that doing so will delete the database of the emails you have marked as spam. The POP3 option sends you a spam report daily if requested. The virus tab informs you that all your incoming and outgoing emails and attachments are automatically scanned for security threats, this provider uses Symantec. You can filter your emails. The additional email account requested at sign up, could aid in security protection and the provider recommends adding it so that they could send you your password in case you forget. GMX mail has an app but not a chat system. When users forget their password, they will input email address answer a question about their identity and the security question and they could choose a new password.

3.4 Risk Analysis

Table 3.2 summarizes the characteristics of the five providers and allows better comparison. Considering the account creating process, the one page account creation in Yahoo and Google presents the hazard that an attacker can easily place himself/herself at a distance closed enough to get all the information needed for identity theft. The multi pages process allow the user to hide information previously entered. Also the security questions in AOL for example seems very weak and common to any other web account services out there and it does not have the option of inputting your own question. Yahoo seems to do a better job with that feature. Google however do not ask for any security question at the time of account creation.

It is interesting to see that while the use of the same password across multiple domains is rated as less secure and creating the “domino-effect” [55], providers do not hesitate to use the same set of security questions among themselves. A user, who truthfully inputs their answer, will be at risk once an attacker successfully hack any one of their accounts; the attacker will be able to enter any other account of their choice.

Whenever an alternative email address is required with a security question, if the password recovery process only requires one of these data, attackers could easily hack additional email accounts by sending other password requests to the account they currently control.

Yahoo accepts qwerty whereas AOL does not. AOL does not require a number of characters for security question answer.

It is very interesting that providers display all your choices after your signing process. For example Yahoo and AOL display your username, security questions and their answers with an option for the user to print, but also for the attacker to copy. In addition having the answers to your questions combined with your email address on paper presents a high risk if anyone retrieves that sheet. Security questions are as important as the password because they are used for password retrieval. The answer is not encrypted when the user is filling in their information. This means that at any time an attacker could read, off the screen, the question and answer.

When you receive a new email in Gmail you can automatically open it. It is up to the user to decide which email to open. In contrast, any attachment in Yahoo is required to be analyzed with antivirus software before opening. Even though Gmail automatically scans attachments and emails for threats, the visual steps that Yahoo and AOL show when analyzing attachments could make the users feel more secure.

Table 3.2 Summary of the Five Email Providers Characteristics

Stages	Attributes	Characteristics	AOL	Gmail	GMX	Hotmail	Yahoo
Setup stage	Steps for account creation	One interface	Multiple interfaces	One interface	One interface	One interface	One interface
		Multiple interfaces					
	Password sophistication	Length	6	8	8	8	6
		Strength	No requirement	No requirement	No combination	Two combination	No requirement
	Security questions	How many questions options	13	6	9	6	10
		How good are the options	General knowledge	Knowledge of information	General knowledge	General knowledge	Knowledge of information
		How many options required	1	0	1	2	2
		Combination(questions/phones/email) required, only questions or no requirement	Only questions	No requirement	Only questions	Combination	Only questions
		Minimum requirement for security question answer	None	None	None	5	4
		Display security questions & answers after sign up is complete	Yes	No	No	No	Yes
		Number of requirement for recovery	3	2	3	2	3
Usage stage	Spam blocking	Automatic spam filtering	Yes	Yes	Yes	Yes	Yes
		Spam reporting	Yes	Yes	Yes	Yes	Yes
	Email address blocking	Presence or absence of feature	Yes	No	Yes	Yes	Yes
	Incoming emails filtering	Presence or absence of feature	Yes	Yes	Yes	Yes	Yes
	Email	Unlimited	Unlimited	10,303 MB	Unlimited	Unlimited	Unlimited

	account storage capacity	10,303 MB					
	Chat system	Presence or absence of feature	Yes, AIM	Yes	No	Yes, MSN Messenger	Yes, Yahoo Messenger
	Mobile app	Presence or absence of feature	Yes	Yes	Yes	Yes	Yes
	Connected to other apps	Presence or absence of feature	No	Yes	No	Yes	Yes
	Password encryption	HTTPS	Yes	Yes	Yes	Yes	Yes
	Scan incoming and outgoing mails for threats	Presence or absence of feature	Yes	Yes	Yes	Yes	Yes
	Attachments view options	Automatic analysis	Automatic	Automatic	Automatic	Automatic	Automatic
		No analysis					

3.4.1 Ranking Methodology

Many authors such as Bones [34] and Karabacak [17] used risk matrix for assessing security risks. We used the following risk matrix, in table 3.3 for analysis, based on the risk level matrix mentioned by Stoneburner et al. [35] regarding information technology systems risk management.

Table 3.3 Risk Matrix

Likelihood of occurrence	Negative impact		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

3.4.2 Rationale for Analysis

3.4.2.1 Ranking Attributes

We judged the importance of the attributes among themselves in terms of their likelihood to occur. At the usage stage,

- Low likelihood attributes are email address blocking, mobile app. These choices were based on the fact that users could block email addresses by reporting them as spam or filtering them to go to trash or other folders. Also, not every user utilizes mobile apps and when they do, cell phones or tablets are mostly used by one individual and cannot carry a lot of data.
- Medium likelihood attributes are connection to other apps with other companies, email storage capacity and chat system. These attributes were classified as medium attributes because they could cause a greater damage and also users had to use them extensively in order for the damage to occur.
- Highly likely to impact security are incoming email filtering, spam blocking system; scanning all incoming and outgoing emails, attachments view options and password encryption. These attributes do not depend on user choices and are associated with a secure use of any email account.

The setup stage attributes were considered as important as the usage stage in terms of security of email accounts. Any flaws observed at that stage endangered the user information as well as the existence of the account. Furthermore security questions were rated as high as password sophistication, because they are the alternatives if the hacker could not guess the user’s password. Then the user password is rated higher than the number of interfaces in account creation because in the case of number of screens, the attackers would need to be present at the time of the registration in order to seize the user's information.

3.4.2.2 Ranking Characteristics

The characteristics were ranked based on their impact on security, therefore:

- The steps for creating email account comprises of one or multiple interfaces. The authors argued that the higher the number of interfaces, the higher the security
- The password length is divided as follow with increasing security:
    - No length requirement or less than 4
    - Minimum of 8 or less
    - Minimum of 9 or more

This classification is based on the literature that shows an advantage of passphrases or sentences over password. "The Federal Information Processing Standard (FIPS) (1985) on password usage is one of the earliest set of guidelines for creating strong passwords; it states that passwords should be approximately five to eight characters long" [55]

- The password strength, according to the literature is more secure if it contains letters, numbers and digit. Thus the security increases with the complexity of the combination. Thus no requirement has low security, any two combination has a medium security and combination of three has a high security
- In regard to the number of questions; the authors posited that a larger set of questions options give a greater chance to achieve a higher level of security.

- Questions which rapport to general knowledge such as birthplace, pet’s name, make of car are considered low in security, anyone could find their answers or these questions are commonly used for authentication. Similarly information which could be obtained from the user easily such as library card number, frequent flyer number, favorite author, favorite book are considered of low security; however since they require that the attacker reads the information or ask someone the information, the authors argue that they are medium in security; acquaintances can find their answers. Any other security questions are considered high in security.
- Security increases as the number of questions required increases.
- A combination of security options was considered to be more secured than only security questions and even more secured than no requirement at all.
- Even though answers to security questions are not passwords, they can help users gain access to their account. Thus according to [55], a minimum of five characters was considered high in security and no requirement was considered low.
- For account password recovery we examined the number of requirement, the higher the better for security.
- The password encryption ratings are based on the literature with https encryption as the best for security.
- The presence or absence of all the other characteristics represents respectively a positive and negative security impacts.

3.4.2.3 Risk Tables for Analysis

We proceeded to create a risk matrix for every attribute according to the previous rating. Table 3.4, table 3.5, table 3.6, table 3.7, table 3.8 and table 3.9 show the risk level based on the ranking of each attribute and its characteristics. For characteristics where we do not have any literature to indicate the rankings, we rated the characteristics across providers. As an example, for the number of characters of a security answer we considered all the providers with none, four or five characters requirement and we gave the highest security impact to the provider with no requirement. When only two characteristics are available, we evaluated the risk as high or low. Finally, we used cumulative risk to assess the risk associated with each provider.

Table 3.4 Risk Values for Account Creation Steps

Attributes		Steps for account creation
Characteristics	Rank	Medium
One interface	High	Medium
Multiple interfaces	Low	Low

Table 3.5 Risk Values for Password Sophistication

Attributes		Password sophistication
Characteristics	Rank	High
No Length requirement or <5	High	High
8>=Length>=5	Medium	Medium
Other Length	Low	Low
No combination or no requirement	High	High
Two combination	Medium	Medium
Combination of three	Low	Low

Table 3.6 Risk Values for Security Questions

Attributes			Security questions
Characteristics		Rank	High
How many questions options	Three questions or Less	High	High
	Four to seven questions	Medium	Medium
	More than 8	Low	Low
How good are the options	General knowledge	High	High
	Knowledge of information	Medium	Medium
	Secure knowledge	Low	Low
How many options required	No requirement	High	High
	One question required	Medium	Medium
	More than two	Low	Low
Type of requirement	No requirement	High	High
	Only questions required	Medium	Medium
	Combination(questions/phones/email) required	Low	Low
Minimum requirement for security question answer	No requirement	High	High
	4 or less	Medium	Medium
	5 or more	Low	Low
Display security questions & answers after sign up is complete	Yes	High	High
	No	Low	Low
Number of requirement for recovery	2 or less	High	High
	3	Medium	Medium
	More than 3	Low	Low

Table 3.7 Risk Values for Email Account Storage Capacity

Attributes		Email account storage capacity
Characteristics	Rank	Medium
Unlimited	High	Medium
10,303 MB	Low	Low

Table 3.8 Other Risk Values

Attributes		Automatic spam filtering (H), spam reporting (H), email address blocking (L), incoming email filtering (H), https encryption (H), scan incoming and outgoing mails for threats (H), automatic analysis of attachments (H)		
Characteristics	Rank	High	Medium	Low
Absence has a greater impact on risk (no)	High	High	Medium	Low
Presence has a lesser impact on risk (yes)	Low	Low	Low	Low

Table 3.9 Risk Values for Chat System, Mobile App and Connection to other Apps

Attributes		Chat system(M), mobile app (L), connection to other apps (M)		
Characteristics	Rank	High	Medium	Low
Presence has a greater impact on risk (yes)	High	High	Medium	Low
Presence has a lesser impact on risk (no)	Low	Low	Low	Low

3.4.3 Reality Analysis Risk Table

The reality analysis risk table 3.10 displays the results of our classification and table 3.11 presents a count of the different risk levels.

Table 3.10 Reality Analysis Risk Table

Stages	Attributes	Characteristics	AOL	Gmail	GMX	Hotmail	Yahoo
Setup stage	Steps for account creation	One interface	Low	Medium	Medium	Medium	Medium
		Multiple interfaces					
	Password sophistication	Length	Medium	Medium	Medium	Medium	Medium
		Strength	High	High	High	Medium	High
	Security questions	How many questions options	Low	Medium	Low	Medium	Low
		How good are the options	High	Medium	High	High	Medium
		How many options required	Medium	High	Medium	Low	Low
		Type of requirement	Medium	High	Medium	Low	Medium
		Minimum requirement for security question answer	High	High	High	Low	Medium
		Display security questions & answers after sign up is complete	High	Low	Low	Low	High
		Number of requirement for recovery	Medium	High	Medium	High	Medium
Usage stage	Spam blocking	Automatic spam filtering	Low	Low	Low	Low	Low
		Spam reporting	Low	Low	Low	Low	Low
	Email address blocking		Low	Low	Low	Low	Low
	Incoming emails filtering		Low	Low	Low	Low	Low
	Email account storage capacity	Unlimited	Medium	Low	Medium	Medium	Medium
		10,303 MB					
	Chat system		Medium	Medium	Low	Medium	Medium
	Mobile app		Low	Low	Low	Low	Low
	Connected to other apps		Low	Medium	Low	Medium	Medium
	Password encryption	HTTPS	Low	Low	Low	Low	Low
	Scan incoming and outgoing mails for threats		Low	Low	Low	Low	Low

	Attachments view options	Automatic analysis No analysis	Low	Low	Low	Low	Low

Table 3.11 Counts of Risks Levels

Counts	AOL	Gmail	GMX	Hotmail	Yahoo
Low count	11	10	12	12	10
Medium count	6	6	6	7	9
High count	4	5	3	2	2
Total	21	21	21	21	21

3.4.4 Discussion

The number of low security risks is superior to all the other categories; however the high and medium security risks counts are equally large. Hotmail and GMX appeared to have the highest count of “low” security risks and gmail had the highest count of high risks. In general there was no large difference among the counts of low, high and medium risks across providers. For the low, medium and high risk counts, all the providers were one or two counts below, above or equal to the median of 11, 6 and 3 respectively. However, for the low counts, AOL was at the median, Gmail and Yahoo were one count below the median; GMX and Hotmail were one above the median. Overall, Gmail had the highest count of high risk which implied google email accounts were at the highest risk of security breach with high impact, however Gmail has the lowest count of low risks implying that there were many steps in placed to avoid risks with low impacts. AOL and GMX followed respectively with the number of high risk counts being four and three but AOL had a lower count of low risks compared to GMX. Hotmail and Yahoo finished the ranking with equal high risks counts of two but Yahoo had a lower count of low risks than Hotmail. Taking into account the medium risks counts, Yahoo came in first position; Hotmail followed with seven medium risks and AOL. Gmail and GMX had equal number of medium risks.

Overall the risk level is increasing as providers changed from Yahoo, Hotmail, GMX, and AOL to Gmail for high severity risks. For medium severity risks, the level increases from Gmail, AOL, GMX, Hotmail to Yahoo and the low counts helped determine the order for risk level counts with a tie.

In conclusion, there is no clear difference on all the high, medium and low security risk counts. There are still areas of improvement for each provider; competition and technology and new researches can allow the free web services to blossom into a more secured system.

Chapter 4: User Perception of Email Accounts

4.1 Risk Analysis Method

A risk assessment tries to answer the following questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

Various risk analysis methods have been applied to the context of information security by developing a list of the critical information security risk factors and analyzing their criticality [48, 59]. The risk analysis method we selected is Information Security Risk Analysis Method (ISRAM). ISRAM is a validated paper-based method developed by Karabacak and Sogukpinar [17] in 2005. It is a survey-based quantitative approach used to analyze the security risks of information technologies. This method was developed as an alternative to complex calculations in previous risk analysis models, to their complex scenarios with a lot of unknowns and to the lack of data often faced when estimating risk. It is also a preferred option to the qualitative methods that often lead to subjective and inconsistent results and are based on the reasoning of the people involved in the analysis. ISRAM allows the participation of all humans involved in the system, offers flexibility in its risk analysis as opposed to software based models which have a rigid frame that limit the amount of variations that can be performed in risk analysis.

ISRAM, as a quantitative method, calculates the risk as a function of the probability of occurrence and consequence of occurrence of a security breach. There are seven steps in ISRAM with the first four occurring before the survey (the fifth step) and the last two after the survey. The survey consists of questions and answer choices related to the information security problem under study. Karabacak et al. recommends that managers, directors, technical personal and common computer users take the survey [17]. Conducting the survey will permit an understanding of the effect of the information security problem by including the perception of actual users.

We chose this methodology because it incorporates a survey methodology for inclusion of the user and also a reliability method for the calculation of the risk. Risk is the probability of occurrence multiplied by the consequences of occurrence. ISRAM is a risk analysis model that can be implemented in a reasonable time frame and allows the participation of the system users [17]. ISRAM was also chosen because of its pertinence as a risk assessment model in information security and its ease of repeatability. In this model, risk is defined as follow in formula 4.1 and formula 4.2. Figure 4.1 shows the ISRAM flow diagram.

Risk= Probability of occurrence of security breach x Consequence of occurrence of security breach (4.1)

Furthermore,

$$Risk = \left(\frac{\sum_m [T_1(\sum_i w_i p_i)]}{m}\right)\left(\frac{\sum_n [T_2(\sum_j w_j p_j)]}{n}\right) \quad (4.2)$$

Where i and j respectively represent the number of questions for the survey of probability and consequences of occurrence of a security breach determined at step 2; m and n respectively represent the number of participants who participated in the survey of probability and consequences of occurrence of a security breach, which becomes definite at step 5;

(w_i, p_i) and (w_j, p_j) respectivelty (weight, numerical value of answer choice) for questions i and j

T_1 and T_2 respectively represent risk tables for the survey of probability and consequences of occurrence of a security breach, constructed at step 4.

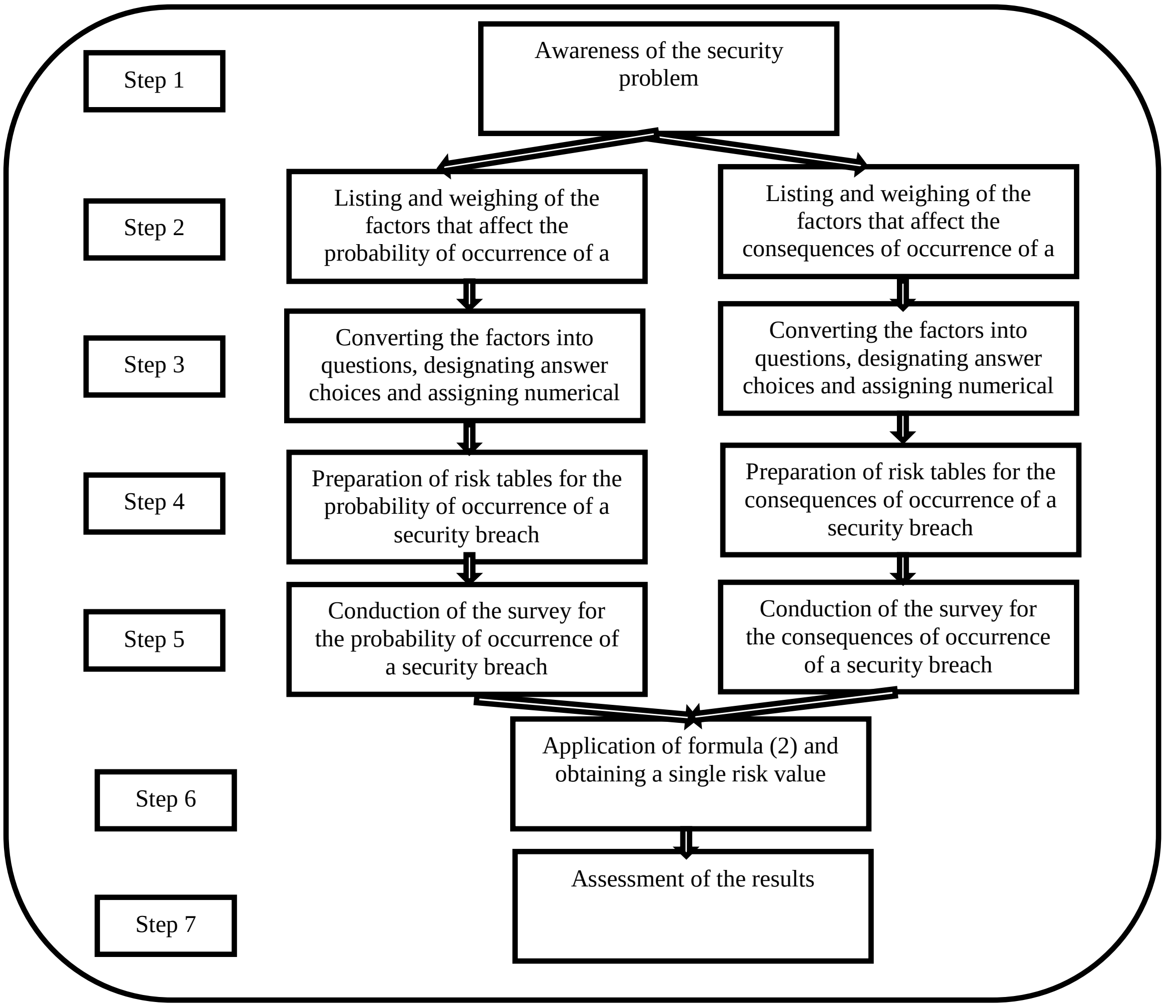
Step 1
Awareness of the security problem
Step 2
Listing and weighing of the factors that affect the probability of occurrence of a
Listing and weighing of the factors that affect the consequences of occurrence of a
Step 3
Converting the factors into questions, designating answer choices and assigning numerical
Converting the factors into questions, designating answer choices and assigning numerical
Step 4
Preparation of risk tables for the probability of occurrence of a security breach
Preparation of risk tables for the consequences of occurrence of a security breach
Step 5
Conduction of the survey for the probability of occurrence of a security breach
Conduction of the survey for the consequences of occurrence of a security breach
Step 6
Application of formula (2) and obtaining a single risk value
Step 7
Assessment of the results

Figure 4.1 ISRAM Flow Diagram

4.2 Application of ISRAM Steps

We were not able to get in touch with the authors in [17] to get a sample survey for the case study. Therefore, we came up with our own survey based on the few examples of the original paper. In the pre-survey phase, we listed the factors associated with the probability and consequences of occurrence of a security breach, determined the number of questions and their weight values, the answer choices and their weight values and finally prepared the risk tables. After conducting the survey, we calculated the risk values and analyzed the results.

4.2.1 Step 1: Awareness of the Problem

There are many providers of free email accounts on the internet. Many users and particularly people at the university rely heavily on these email accounts as a mean of communication. There have been many reports of accounts being hacked, private or personal information being divulgated due to unsecure email communication. The email providers have in place many security settings to protect their users but the users' perceptions and knowledge of security also influence the risk level they are subject to. A methodical analysis is thus needed to assess the relationship and disparity between the reality of the security of an email account and the users' perceptions. Students usually have several email accounts from different providers which are subject to an attack in which personal information can be disclosed or stolen, accounts can be compromised and privacy lost. This analysis will help explore the risk level of the different email providers used by students. This completes the first step of the ISRAM risk analysis.

4.2.2 Step 2 : List and Weight Factors

First, we identified twenty two factors which affect the probability of occurrence of a security breach of an email account. Some of those factors are password length, password complexity, security questions strength, types of website entered, number of files downloaded per day, number of attachments received, number of new emails per day, spam or junk filtering system, email filtering system, popularity of the email domain and messenger (chat) system. Second, we developed a list of the five factors which affect the consequences of occurrence of a security breach of an email account that comprises sharing of emails, sharing of attachments, importance of files in email account, type of files, and volume of outgoing emails. Additionally some factors, such as seniority of the email account and the type of device used for email access, might affect both the probability and consequences of occurrence of a security breach of an email account; the total number of these factors was twelve.

Based on the rationale behind the reality analysis, we attributed weights to the factors for probability and consequence of occurrence of a security breach. The other factors, which do not appear in the reality analysis, were given a weight based on their level of impact on security. Appendix A presents an explanation for the weight of each question.

Table 4.1 is a reference table for the weights of the factors. We used a table similar to the previous study [17] because it will difficult without a committee of experts to come up with a new tabulation which is not biased by the author's opinion solely. Table 4.2 and table 4.3 display the factors values respectively for the probability and consequences of occurrence of a security breach in email accounts and Table 4.4 contains the factors that affect both probability and consequences as well as their corresponding weights.

Table 4.1 Weight Values and Explanation of the Factors

Weight value	Explanation
3	The factor is directly associated with a severe vulnerability and/or the factor is directly

	associated with a critical asset and/or there is no countermeasure in place. Because of these reasons, the factor is most effective factor that affects the probability of occurrence of a security breach or the consequences of occurrence of a security breach. The factor contributes directly to the value of the risk parameter.
2	The factor is somewhat associated with a vulnerability and/or the factor is directly associated with an important asset and/or there is a few countermeasure in place. Because of these reasons, the factor is slightly/normally effective factor that affects the probability of occurrence of a security breach or the consequences of occurrence of a security breach. The factor contributes somewhat directly to the risk parameter.
1	The factor is a little associated with vulnerability and/or the factor is indirectly associated with an important asset and/or where are enough countermeasures in place. Because of these reasons, the factor is least effective factor that affects the probability of occurrence of a security breach or the consequence of occurrence of a security breach. The factor contributes indirectly to the value of the risk parameter.

According to the reality analysis we developed the following summary in Table 4.1a.

Table 4.1a: Summary Table of Weight Values and Characteristics

Weight Value	Characteristics	Risk in Reality Analysis
3	The factor contributes directly to the value of the risk parameter	High
2	The factor contributes somewhat directly to the risk parameter	Medium
1	The factor contributes indirectly to the value of the risk parameter	Low

Table 4.2 Probability Factors and their Weight Values

Factor	Weight Value
Password length	3
Password complexity	3
Security questions strength	3
Sample security questions	3
Spam filtering system	3
Junk(phishing) filtering system	3
Use of antivirus on hardware device	3
Use of antispyware on hardware device	3
Popularity of the email domain	3
Number of attachments received	2
Type of attachment received	2
Frequency of email use	2
Type of email received	2
Messenger(chat) system	2
Email provider 's reputation	2
Internet experience level	2
Use of storage media	2
Number of new emails per day	1
Number of websites visited	1
Number of files downloaded per day	1
Type of website entered	1
Type of files downloaded	1

Table 4.3 Consequence Factors and their Weight Values

Factor	Weight Value
Sharing of emails	3
Sharing of attachments	3
Importance of files in email account	3
Type of files in email account	3
Outgoing email volume	2

Table 4.4 Factors that Affect both the Probability and the Consequences and their Weights

Factor	Weight Value for Probability	Weight Value for Consequence
Places mailbox is checked	3	3
Update against vulnerabilities	3	3
Access to the shared folders of other computers	3	3
Number of computers which are accessed by sharing	3	3
Use(activities) of email account	3	3
Seniority of email account	2	3
Type of device	2	3
Frequency of update	2	2
Type of user account	2	2
Open email from unknown sender	2	2
Receive email from unknown sender	2	1
Frequency of unknown sender’s email	2	1

The table below is a reference table for the weights of the answer choices. Here again, we use a similar table to the previous study [17] because it will be difficult without a committee of experts to come up with a new tabulation which is not biased based solely on the author’s opinion.

Table 4.5 Numerical Values of Answer Choices

Numerical Value of Answer Choice	Explanation
4	Most effective answer choice. Affect enormously the probability of occurrence of a security breach or the consequences of occurrence of a security breach.

3	Rather effective answer choice. Affect highly the probability of occurrence of a security breach or the consequences of occurrence of a security breach.
2	Somewhat effective answer choice. Affect considerably the probability of occurrence of a security breach or the consequences of occurrence of a security breach.
1	Least effective answer choice. Affect slightly the probability of occurrence of a security breach or the consequences of occurrence of a security breach.
0	No effect on the probability of occurrence of a security breach or the consequences of occurrence of a security breach.

4.2.3 Step 3: Change Factors into Questions, Find Answer Choices and their Values

Our procedure for changing factors into questions is similar to the sample questions provided in Karabacak and Sogukpinar [17] paper. The answer choices also follow the same format than in the original paper. The number of answer choices was selected by the authors as suggested in [17]. The numerical values assigned to the answer choices show the differentiation between the choices.

In our questionnaire, the total number of questions was 47. There were two parts to the survey displayed on two pages. Some questions in our questionnaire (1 and 18 in part I; 1, 7, 10, 16, 17 and 19 in part II) were neither parts of the factors for neither probability nor consequences of occurrence of a security breach; but they helped us determine the characteristics of the participants and their opinion on security issues. Such questions and their answer choices were not included in the risk calculation nor given any weight. Then the total number of questions used in the analysis was 39. The rationale behind the values assigned to the answer choices is provided in appendix A.

One question has seven answer choices, two questions have six answer choices, nine questions have five answer choices and thirteen of these questions have four answer choices; some of these with one option being ‘other, please specify’. Participants input their special answer whenever appropriate. Eight have three answer choices (yes/no/don’t know) and six have two answer choices (yes/No). Table 4.6 shows some sample questions with their answer choices. The letters p and c next to the questions represent respectively the probability or consequences factors and the numbers, their values.

Table 4.6 Sample Questions and Answer Choices

Questions	Answer Choices	Values
Does your email account have a spam or junk filtering system? p3	Yes	1
	No	4
	Don't know	4
Does your email account have a chat system? p2	Yes	4
	No	0
	Don't know	4
How many attachments do you receive per day in your inbox? p3	More than 12	4
	8-11	3
	4-7	2
	Fewer than 3	1
How strong are the security questions of your email account? Note: Security questions are used for password retrieval. p3	Very strong	1
	Strong	2
	Moderately strong	3
	Not strong	4
How would you rate the importance of the files in your email account? c3	Very important	4
	Important	3
	Moderately important	2
	Not important	0
To how many recipients do you send email per day from your email account? c2	More than 16	4
	11-15	3
	6-10	2
	Fewer than 5	1
What do you use your email account for? Note: Please only choose the primary purpose of your email account. p2, c2	Professional	2
	Academic	1
	Social	4

	Shopping	3
	Other (please specify)	other
How often do you receive emails from unknown senders in your inbox? p2, c1	Everyday	4
	Frequently	3
	Not so frequently	2
	Rarely	1
	Never	0

4.2.4 Step 4: Preparation of Risk Tables

The survey results were quantitatively analyzed using risk tables, which link the risk parameter to the results. One table was constructed for the probability and another for the consequences of occurrence of a security breach; they were the main reference points for assessing the survey results.

- We assigned values to the answer choices according to Table 4.5. The list of answer choices and numerical values is provided in appendix A.
- Then the minimum and maximum values which could be obtained from the survey were determined; on the basis that the participant chooses the answers with the lowest and highest values.
- For the probability, the minimum and maximum survey values were 61 and 308 and for the consequence, these values were 27 and 172.
- We sorted the values between the minimum and maximum survey values to correspond to five risk levels by grouping them evenly. As in the original paper, the five levels of probabilities correspond increasingly to very low (1), low (2), medium (3), high (4), very high (5). Accordingly for the consequences, negligible (1), minor (2), important (3), serious (4) and very serious (5). The interval scales are 48 for probability and 28 for

consequences. The intervals for probability/consequences, which were not divided evenly, were assigned to the most critical value. Thus, the interval of ‘very high probability’ was 51 and the interval of ‘very serious consequences’ was 29. Table 4.7 and Table 4.8 show the intervals and their corresponding risk levels.

The fundamental risk formula: Risk = probability x consequence is applied to obtain a risk matrix of Table 4.9. The final risk table is the same as in the original paper [17]. Table 4.9 presents the risk values between 1 and 25, with the range 20 to 25 being of very high probability.

Table 4.7 Risk Table for the Survey of Probability of Occurrence of a Security Breach

Survey Results		Qualitative Scale	Quantitative Scale
Lower Bound	Higher Bound		
61	109	Very low probability	1
110	158	Low probability	2
159	207	Medium probability	3
208	256	High probability	4
257	308	Very high probability	5

Table 4.8 Risk Table for the Survey of Consequences of Occurrence of a Security Breach

Survey Results		Qualitative Scale	Quantitative Scale
Lower Bound	Higher Bound		
27	55	Negligible consequences	1
56	84	Minor consequences	2
85	113	Important consequences	3
114	142	Serious consequences	4
143	172	Very serious consequences	5

Table 4.9 Final Risk Table for the Survey

Risk	1: Very Low	2: Low	3: Medium	4: High	5: Very High
1: Negligible	1: Very Low	2: Very Low	3: Very Low	4: Low	5: Low
2: Minor	2: Very Low	4: Low	6: Low	8: Medium	10: Medium
3: Important	3: Very Low	6: Low	9: Medium	12: Medium	15: High
4: Serious	4: Low	8: Medium	12: Medium	16: High	20: Very High
5: Very Serious	5: Low	10: Medium	15: High	20: Very High	25: Very High

4.2.5 Step 5: Conduct the Survey

The survey was distributed via listserv at the University of Maryland to students in the college of engineering, department of computer science and campus FYI. A period of one week was allowed for students to answer the questionnaire via a link attached to the survey. All participants agreed freely to respond to the survey, no recompense or prizes were given. The survey was pre-tested by three students; semantic and grammar corrections were made accordingly; the final version was verified by the student's advisor.

4.2.6 Step 6: Application of Risk Formula and Obtaining a Single Risk Value

Question 1 in the survey allowed us to collect the different email providers used by the participants. 9.7% used Yahoo, 77.6% used Google, 4.5% Hotmail, and 8.2% used other providers such as Comcast, Juno, Lotus notes, XecuNet, RiseUp, UMD or hosted their own email server. For our analysis, we chose Yahoo, Google and Hotmail which were used in the reality analysis.

Each participant survey responses, with a first choice of Yahoo, Google or Hotmail, were analyzed to find the values of the probability and consequences of occurrence of a security breach and the corresponding T1 and T2 values. For multiple choice questions, the answer choice with the highest value was considered. Hence for

Hotmail, the value associated with the probability of occurrence of a security breach was 2.83, approximately medium probability and the value of the consequence of occurrence of a security incident was 2.67, relatively important consequences; the risk value was 7.56 which is between a low and medium level risk. In addition, the value associated with the probability and consequences of Yahoo users being subject to security breach were equally 3.15 corresponding to medium probability and important consequences; thus the value of the risk was 9.95 which is a medium risk level. Lastly, Gmail had 2.72 as the value associated with the probability of occurrence of a security breach and the value of the consequence was 2.95; therefore the risk value was 8.03 which is a medium risk level. Table 4.10, 4.11, 412 provide the survey results for Hotmail, Yahoo and Gmail respectively; and Table 4.13 provides a summary of the results of the risks.

Table 4.10 Survey Results for Hotmail Users

Participant	Link	Probability Sum(Wipi)	T1	Consequence Sum(Wjpj)	T2
Participant 1	Engineering	179	3	98	3
Participant 2	Engineering	152	2	94	3
Participant 3	Engineering	163	3	83	2
Participant 4	Campus FYI	174	3	82	2
Participant 5	Computer Science	159	3	96	3
Participant 6	Computer Science	169	3	108	3
		Average	2.83	Average	2.67

Table 4.11 Survey Results for Yahoo Mail Users

Participants	Link	Probability Sum(Wipi)	T1	Consequence Sum(Wjpj)	T2
Participant 1	Engineering	208	4	110	3
Participant	Engineering	162	3	94	3

2					
Participant 3	Computer Science	193	3	120	4
Participant 4	Computer Science	159	3	70	2
Participant 5	Computer Science	169	3	96	3
Participant 6	Campus FYI	159	3	113	3
Participant 7	Campus FYI	173	3	96	3
Participant 8	Engineering	181	3	128	4
Participant 9	Campus FYI	193	3	132	4
Participant 10	Campus FYI	173	3	85	3
Participant 11	Engineering	213	4	121	4
Participant 12	Engineering	176	3	80	2
Participant 13	Engineering	172	3	83	3
		Average	3.15	Average	3.15

Table 4.12 Survey Results for Gmail Users

Participants	Link	Probability Sum(Wipi)	T1	Consequence Sum(Wjpj)	T2
Participant 1	Engineering	146	2	73	2
Participant 2	Engineering	179	3	109	3
Participant 3	Engineering	170	3	106	3
Participant 4	Engineering	180	3	107	3
Participant 5	Engineering	182	3	87	3
Participant 6	Engineering	215	4	99	3
Participant 7	Engineering	204	3	148	5
Participant 8	Engineering	200	3	111	3
Participant 9	Engineering	206	3	115	4
Participant 10	Engineering	159	3	111	3
Participant 11	Engineering	161	3	104	3
Participant 12	Engineering	168	3	94	3
Participant 13	Engineering	210	4	153	5
Participant 14	Engineering	144	2	87	3
Participant 15	Engineering	172	3	99	3
Participant 16	Engineering	172	3	107	3

Participant 17	Engineering	168	3	98	3
Participant 18	Engineering	175	3	126	4
Participant 19	Engineering	169	3	118	4
Participant 20	Engineering	191	3	121	4
Participant 21	Engineering	130	2	83	2
Participant 22	Engineering	163	3	99	3
Participant 23	Engineering	176	3	107	3
Participant 24	Engineering	171	3	121	4
Participant 25	Engineering	228	4	133	4
Participant 26	Engineering	192	3	133	4
Participant 27	Engineering	182	3	119	4
Participant 28	Engineering	187	3	106	3
Participant 29	Engineering	149	2	103	3
Participant 30	Engineering	151	2	67	2
Participant 31	Engineering	140	2	70	2
Participant 32	Engineering	172	3	101	3
Participant 33	Engineering	155	2	106	3
Participant 34	Engineering	204	3	112	3
Participant 35	Engineering	160	3	98	3
Participant 36	Engineering	195	3	125	4
Participant 37	Engineering	179	3	117	4
Participant 38	Engineering	179	3	114	4
Participant 39	Engineering	193	3	127	4
Participant 40	Engineering	152	2	87	3
Participant 41	Engineering	183	3	121	4
Participant 42	Engineering	161	3	90	3
Participant 43	Engineering	167	3	122	4
Participant 44	Engineering	168	3	100	3
Participant 45	Engineering	166	3	99	3
Participant 46	Computer Science	159	3	106	3

Participant 47	Computer Science	137	2	61	2
Participant 48	Computer Science	152	2	69	2
Participant 49	Computer Science	216	4	137	4
Participant 50	Computer Science	134	2	66	2
Participant 51	Computer Science	159	3	95	3
Participant 52	Computer Science	167	3	80	2
Participant 53	Computer Science	173	3	109	3
Participant 54	Computer Science	163	3	114	4
Participant 55	Computer Science	174	3	104	3
Participant 56	Computer Science	161	3	80	2
Participant 57	Computer Science	182	3	80	2
Participant 58	Computer Science	153	2	95	3
Participant 59	Computer Science	200	3	97	3
Participant 60	Computer Science	152	2	101	3
Participant 61	Computer Science	149	2	70	2
Participant 62	Computer Science	146	2	95	3
Participant 63	Computer Science	192	3	87	3
Participant 64	Computer Science	129	2	60	2
Participant 65	Computer Science	163	3	76	2
Participant 66	Computer Science	140	2	78	2
Participant 67	Computer Science	175	3	102	3
Participant 68	Computer Science	133	2	55	1
Participant 69	Computer Science	175	3	92	3
Participant 70	Computer Science	189	3	110	3
Participant 71	Computer Science	176	3	112	3
Participant 72	Computer Science	144	2	72	2
Participant 73	Computer Science	175	3	108	3
Participant 74	Computer Science	165	3	118	4
Participant 75	Computer Science	127	2	61	2
Participant 76	Computer Science	151	2	70	2

Participant 77	Computer Science	128	2	58	2
Participant 78	Computer Science	140	2	65	2
Participant 79	Computer Science	158	2	100	3
Participant 80	Computer Science	154	2	56	2
Participant 81	Computer Science	177	3	104	3
Participant 82	Computer Science	160	3	110	3
Participant 83	Computer Science	179	3	90	3
Participant 84	Computer Science	175	3	112	3
Participant 85	Computer Science	169	3	101	3
Participant 86	Computer Science	178	3	91	3
Participant 87	Computer Science	141	2	71	2
Participant 88	Computer Science	192	3	109	3
Participant 89	Computer Science	173	3	112	3
Participant 90	Computer Science	149	2	79	2
Participant 91	Campus FYI	189	3	99	3
Participant 92	Campus FYI	141	2	66	2
Participant 93	Campus FYI	151	2	74	2
Participant 94	Campus FYI	205	3	107	3
Participant 95	Campus FYI	193	3	117	4
Participant 96	Campus FYI	155	2	110	3
Participant 97	Campus FYI	207	3	128	4
Participant 98	Campus FYI	148	2	113	3
Participant 99	Campus FYI	156	2	88	2
Participant 100	Campus FYI	223	4	137	4
Participant 101	Campus FYI	157	2	85	3
Participant 102	Campus FYI	147	2	81	2
Participant 103	Campus FYI	167	3	75	2
Participant 104	Campus FYI	188	3	94	3
		Average	2.72	Average	2.95

Table 4.13 Risk Values across Providers

Providers	Probability value	Consequence value	Risk
Hotmail	2.83	2.67	7.56
Gmail	2.72	2.95	8.03
Yahoo	3.15	3.15	9.95

4.2.7 Step 7: Assessment of the Results

The risk value associated with each email provider is the single most important output of ISRAM; it is obtained taking into consideration the system under study but also the human in the system. Our analysis included 123 people divided between 28 females and 95 males. 42.3% were graduate students, 17.1% were senior, 6.5% junior, 12.2% sophomore, 13.8% freshman and 8.1% were staff, faculty, employee or post doc. The largest percent of our participants were students with some experience using computers and 64.2% of them owned a laptop while 68.3% were heavy internet users. About 71% of the participants revealed that their email accounts were "very important" to them. From this risk analysis, important results were obtained. Based on perception, participants believed that all the providers had a medium risk level, with Hotmail having the lowest risk, followed by Gmail and Yahoo being less secure. It is interesting to note that for Gmail, as seen in Table 4.14, participants with engineering background believed that they were more at risk than participants from computer science. This could be explained by the facts that computer science students believed they have higher security settings than engineering students.

Table 4.14 Gmail Risk level based on participant major

Major	Value of Probability	Value of Consequence	Risk
Engineering	2.89	3.31	9.57
CS	2.6	2.62	6.82

Questions 10 surveyed users on their perception of some commonly used security questions. Question 10 was a Likert-type scale question with four dimensions from very strong to not strong. Figure 4.2 presents the distribution of the survey results for each security question. Of all the proposed questions, only the security question "in which city did your parents meet" was rated as "very strong" by the highest number (33.6%) of all the 134 participants. Also, the majority of the participants believed that "what is your mother's maiden name" and "what city were you born in" were "not strong" security questions.

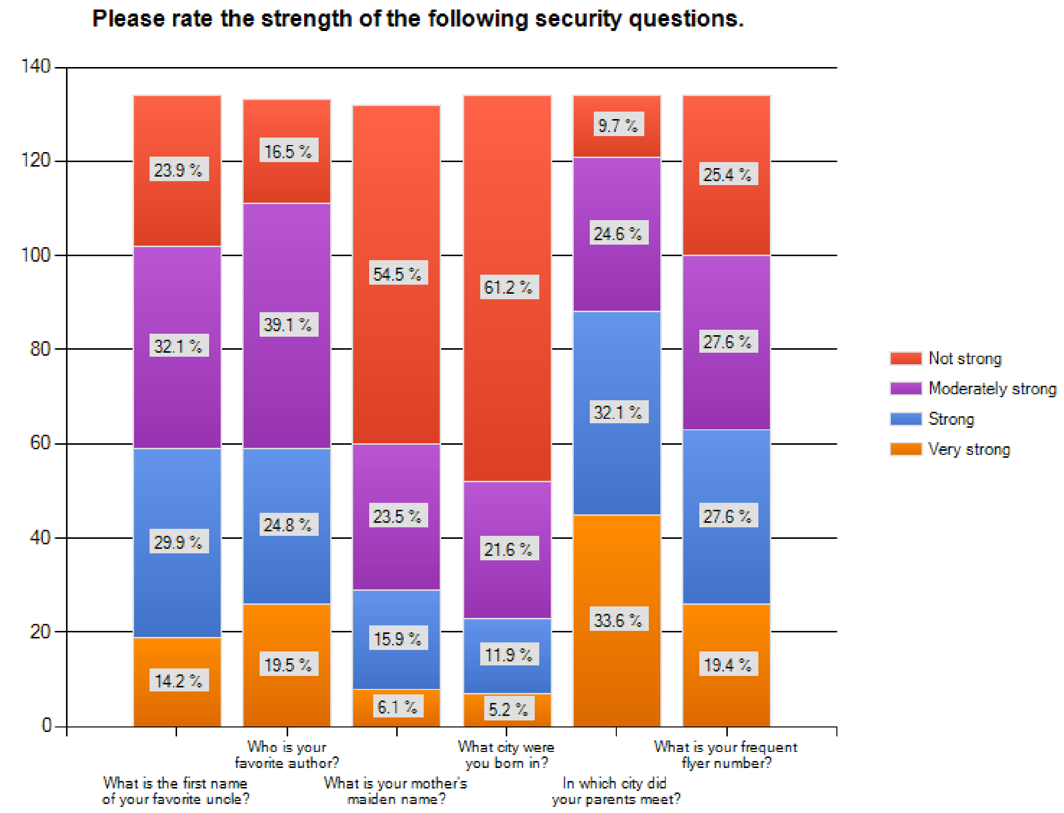

Figure 4.2 Users Perceptions on Security Questions

Since our study took place in an academic environment, we utilized the opportunity to rate the security of the university account versus the free account of the participant’s provider. Of the 123 participants, 68.9% asserted that their security questions/answers for my university email account are very strong and 86.8% said that their university email password is very strong. However only 25.3% of participants felt more secure using a university email account than their provider email account, furthermore just 12.6% believed that their university email account can never be hacked.

And then 78.9% preferred to use their university email account while 59.8% forwarded their university account emails to their personal email provider account. The strength of the university security questions and password led to a preference in using the university account, but the perception of the users on the security of their accounts and their protection from hackers contradicts the above statement. Interestingly, more than half of those participants (61.8%) have between two and three email accounts which might increase their risk levels if we were to combine the probability and consequences of occurrence of a security breach of those accounts together. 21.1% have between 4 and 5 accounts and 4.9% have more than six accounts. Only 12.2% use one account, which might be the proportion for which this analysis relates more closely to.

4.3 <u>Discussion</u>

The reality analysis suggests that Gmail has the highest count of high risk and Hotmail and Yahoo have the same count of high risk. Yahoo has the highest count of medium risk, followed by Hotmail and Gmail. Hotmail has the highest count of low risk and Yahoo and Gmail have the same count of low risk. Alternatively, the perception analysis revealed that Yahoo has the highest level of risk, followed by Gmail and Hotmail. All Hotmail users believed that their email provider is popular because it is now an “integrated part of Windows 8”, old and well-known and it is “pushed by several internet providers.” In addition, one participant asserted that since Hotmail migrated to Outlook.com it has not been hacked; thus Hotmail has a good reputation. The low security risk associated with Hotmail is based on the facts that none of the participants open mails from unknown senders, they rarely open emails from unknown senders, the majority of them use their account for professional and academic purposes, they only send emails to fewer than 5 recipients per day, they do not use public network for email access and most of them believed that a good password is 9 characters long and above and the use of combination of letters and number and non-letters, not numbers in a password is a good password complexity. However, the reality analysis showed that whilst Hotmail had recently moved towards stringer requirements that their account recovery process is still very weak. Also, participants reported receiving mails from unknown senders which leads to believe that the junk filtering system of Hotmail might not be quite effective. In addition, some of the participants do not know whether their account had a message filtering system even though all of the respondents had their accounts for 5 years or more. Their perception of their account security might be biased from their lack of knowledge. Additionally, Hotmail users rated the security questions “what is the name of your favorite uncle”, “who is your favorite author”, “in which city did your parents meet” and “what is your frequent flyer number” as “very strong.” But these security questions are general questions that anyone could find out if they are a little familiar with the users. For example, the frequent flyer number is usually on every flight ticket and usually the card lies on the table at home. Furthermore, most of Hotmail users rated “what is your mother’s maiden name as “strong”. Yet, most people typically have their mother maiden name as middle name and it should also be noted that this particular question that was rated as strong by Hotmail users is used across multiple websites, thus creating a domino-effect as mentioned in the reality analysis.

Yahoo users answered that many people have email accounts with yahoo and that they were very few “large scale hacking” scandals. But the highest risk associated with Yahoo mail is that the majority of users receive more than 18 new emails per day in their inbox including personal emails and advertisement; this exposes them to a greater risk of scam or phishing attacks. Most of them were aware that their email accounts had a chat system, which led to the conclusion that they used it and therefore could be victims of fraud through the messaging system as well. In addition, more than half of the users send emails to multiple recipients. Thus if an attacker gets hold of one of those emails, there are lots of opportunities for phishing scams since the attacker can portray as anyone in the email. The majority of the users also stored their personal information mostly rated as “important” in their account which makes them vulnerable. Furthermore, they used their account for social and academic purposes mostly. According to the weights, since the social use exposes to the greater risk, this contributes to the high risk level associated with Yahoo. All users open their emails at home but some of them used public library and public network; these options present a higher threat to their security considering that they also shop and visit social website online. Yahoo users rated “what is your frequent flyer number” as not strong, “what city where you born in” and what is your mother’s maiden name” equally, with some people rating them as moderately strong and some others not strong. The security questions “What is the first name of your favorite uncle” and “in which city did your parents meet” were considered very strong by the majority of the users.

In contrast to the previous two providers, most Gmail users did not rate any of the security questions as very strong. In fact, “what is your frequent flyer number”, “What is the first name of your favorite uncle” and “in which city did your parents meet” were rated as strong, “who is your favorite author” was rated as moderately strong and “what city where you born in” and what is your mother’s maiden name” were rated as not strong. These ratings are more closely related to the reality analysis since all of these questions could be classified as general knowledge or knowledge of information. Almost all participants asserted that Google was very popular because

- of its innovation when it first came out;
- all of their friends have Gmail;
- many universities including UMD use Gmail;
- Google has many useful features such as Google docs, chat and phone;
- Google is a popular search engine; it’s user friendly; the interface is simple and finally;
- Google is the industry leader.

Many of these aforementioned characteristics also led Gmail users to believe that Gmail has a good reputation since they rarely hear that Gmail accounts had been hacked in comparison to Yahoo. Users believe Gmail has very good security procedures like the two-step accounts verification, and the use of https and a spam blocking feature which works. Even with all the perception on the security of Gmail, most users answered that their security questions were “moderately strong.” Thus the existence of security features does not directly lead to the implementation of these features even when the users perceive the value added of the features. Most users receive more than 18 emails per day and also store their personal information in their email accounts. Almost every user opens their email at home but some also at the public library or on public network; almost half of the participants use their Gmail accounts for shopping and on social websites.

Clearly the perception of the users differ considerably when it comes to security and security questions, which translates into the different levels of risk attributed to each provider. In summary, there is not an agreement between the reality analysis and the perception analysis.

Chapter 5: Conclusions

5.1 Limitation

The perception analysis depended greatly on the understanding of the questions. Even though we strived to make them as clear as possible, there were still some misconceptions from a few participants. As examples, some participants stated they do not receive email from unknown senders but when asked about the frequency of reception of emails from unknown senders, they chose rarely or not so frequently instead of never. Similarly, some participants stated they have access to shared folders of other computers but they selected not applicable when questioned on the number of computers accessed by sharing.

The security questions and their answers were critical in this analysis. Though it may seem right to categorize the questions based on their forms (general knowledge, knowledge on information or knowledge on security), this assumes that people answer the questions objectively because some users can input random answers. For instance, one participant answered their security questions by generating random codes from computer software.

Another limitation of this study is that some participants do not use antivirus or anti-spyware because they run their computers on Linux. The analysis did not give them any credit for that given that we did not ask for the operating system in the questionnaire.

As mentioned earlier in the reality analysis, the ranking of the providers was based on their settings and requirements at the time of our study. These settings and requirements change continuously, thus there is a need of repeatedly evaluating the risk associated with each provider.

5.2 Conclusion

The future of email is tenuous without a general climate of online trust. Hence, building and sustaining user trust on the Internet present an ongoing challenge for providers and is a research topic of increasing interest and importance. Even though, the perception analysis gave a ranking of the providers, the reality analysis could not be as distinctive. There were some trade-offs to consider because no provider came across with all low counts on all levels of risk.

Even when an interface is optimized to induce trust, the security and benefits of email will still require an educated user who is informed about the risks and protections that are present. Authentication processes are really important in email security. Studies (21, 60, and -20) on authentication methods have shown that users preferred usability, convenience over security even when they know their choice reflects a greater risk. This perception will remain unchanged until their perception of threat raise to a limit where authentication processes become important [20] or until they are subjects of attack. Our analysis confirms that users' perceptions on authentication processes are often not realistic, thus they believed their email accounts are less at risk than it actually is.

The security of email accounts was analyzed in terms of security of communication through the Internet, thus the privacy and policies of the different providers were not analyzed in this study. However, it is important to note that all the providers had some terms of use, privacy statement or policies that the users agree to before creating their accounts.

5.3 Future Works

Many email providers offer the possibility for users to link their different email accounts together or access their account from another interface. This is an interesting phenomenon which reduces users' time login into different accounts. It would be interesting to research the impact of that combination on the security of those email accounts and the users' information given that each provider has different settings available.

The perception analysis allowed us to briefly investigate the effects of domain (.com and .edu) on online trust and security. More research is needed in this area and could include .com, .edu, .net and .org domains.

Appendix A

QUESTIONS	To Be Determined?	ANSWERS	SURVEY QUESTION	ANSWER CHOICES	SCORES	COMMENTS
q1	Skipped		Who is your email provider? Note: If you have many providers, please only choose the one you use the most and/or daily.		Skipped	
q2		a1	Do you think that your email provider is popular?	Yes	4	If popular more victims from attacker's point of view.
q2		a2	Do you think that your email provider is popular?	No	1	Risk reduced but not 0.
q2		a3	Do you think that your email provider is popular?	Don't know	4	Assume worst.
q3		a1	Do you think that your email provider has a good reputation?	Yes	1	Attackers fear sanctions or being caught or want to break in.
q3		a2	Do you think that your email provider has a good reputation?	No	4	
q3		a3	Do you think that your email provider has a good reputation?	Don't know	4	
q4		a1	Do you use your email daily?	Yes	4	Direct association with asset.
q4		a2	Do you use your email daily?	Most of the time	3	
q4		a3	Do you use your email daily?	No	2	
q5		a1	How many attachments do you receive per day in your inbox?	More than 12	4	Affects enormously the probability
q5		a2	How many attachments do you receive per day in your inbox?	8-11	3	
q5		a3	How many attachments do you receive per day in your inbox?	4-7	2	
q5		a4	How many attachments do you receive per day in your inbox?	Fewer than 3	1	
q6		a1	How many new emails do you receive per day in your inbox?	More than 18	4	

q6		a2	How many new emails do you receive per day in your inbox?	12-17	3	
q6		a3	How many new emails do you receive per day in your inbox?	6-11	2	
q6		a4	How many new emails do you receive per day in your inbox?	Fewer than 5	1	
q7		a1	How strong are the security questions of your email account? Note: Security questions are used for password retrieval.	Very strong	1	
q7		a2	How strong are the security questions of your email account? Note: Security questions are used for password retrieval.	Strong	2	
q7		a3	How strong are the security questions of your email account? Note: Security questions are used for password retrieval.	Moderately strong	3	
q7		a4	How strong are the security questions of your email account? Note: Security questions are used for password retrieval.	Not strong	4	
q8		a1	What type of attachments do you receive in your inbox? Choose all that apply.	Executable	4	Include zip archives.
q8		a2	What type of attachments do you receive in your inbox? Choose all that apply.	Scripts	3	Include Matlab code, PGP & Diff, Music files.
q8		a3	What type of attachments do you receive in your inbox? Choose all that apply.	Documents	1	
q8		a4	What type of attachments do you receive in your inbox? Choose all that apply.	Photos	2	
q8		a5	What type of attachments do you receive in your inbox? Choose all that apply.	Other (please specify)	other	
q9		a1	What type of email do you receive in your inbox? Choose all that apply.	Professional	2	Attackers can fake professional account.
q9		a2	What type of email do you receive in your inbox? Choose all that apply.	Academic	1	Most emails will come from .edu.
q9		a3	What type of email do you receive in your inbox? Choose all that apply.	Personal	3	Attackers can fake being a known person.
q9		a4	What type of email do you receive in your inbox?	Advertisement	4	

			Choose all that apply.			
q9		a5	What type of email do you receive in your inbox? Choose all that apply.	Other (please specify)	other	Depending on the type of email received, probability of attacks increases
q10		a1	Does your email account have a message filtering system?	Yes	1	Reduce probability but not 0 because the user might not use the filtering or not use it properly.
q10		a2	Does your email account have a message filtering system?	No	4	
q10		a3	Does your email account have a message filtering system?	Don't know	4	Assume worst.
q11		a1	Does your email account have a spam or junk filtering system?	Yes	1	Since we cannot measure the effectiveness of the spam blocking feature, this probability is reduced but not 0.
q11		a2	Does your email account have a spam or junk filtering system?	No	4	
q11		a3	Does your email account have a spam or junk filtering system?	Don't know	4	Assume worst.
q12		a1	Does your email account have a chat system?	Yes	4	
q12		a2	Does your email account have a chat system?	No	0	
q12		a3	Does your email account have a chat system?	Don't know	4	
q13		a1	Do you often send emails to multiple recipients?	Yes	4	
q13		a2	Do you often send emails to multiple recipients?	No	0	
q14		a1	Do you often share attachments with multiple recipients?	Yes	4	
q14		a2	Do you often share attachments with multiple recipients?	No	0	
q15		a1	What type of files do you store in your email account? Choose all that apply.	Personal information	4	
q15		a2	What type of files do you store in your email account? Choose all that apply.	Private documents	2	This was analyzed as any type of documents,

						including online storage, homework, reports, and academic documents.
q15		a3	What type of files do you store in your email account? Choose all that apply.	Private photos	3	
q15		a4	What type of files do you store in your email account? Choose all that apply.	Other (please specify)	other	Ads, almost nothing were given a rating of 1.
q16		a1	To how many recipients do you send email per day from your email account?	More than 16	4	
q16		a2	To how many recipients do you send email per day from your email account?	11-15	3	
q16		a3	To how many recipients do you send email per day from your email account?	6-10	2	
q16		a4	To how many recipients do you send email per day from your email account?	Fewer than 5	1	
q17		a1	How would you rate the importance of the files in your email account?	Very important	4	
q17		a2	How would you rate the importance of the files in your email account?	Important	3	
q17		a3	How would you rate the importance of the files in your email account?	Moderately important	2	
q17		a4	How would you rate the importance of the files in your email account?	Not important	0	
q18	Skipped	Skipped	How would you rate the importance of your email account?		Skipped	
q19		a1	Do you receive emails from unknown senders in your inbox?	Yes	4	Can be good or bad.
q19		a2	Do you receive emails from unknown senders in your inbox?	No	0	
q20		a1	How often do you receive emails from unknown senders in your inbox?	Everyday	4	
q20		a2	How often do you receive emails from unknown senders in your inbox?	Frequently	3	
q20		a3	How often do you receive emails from unknown senders in your inbox?	Not so frequently	2	

q20		a4	How often do you receive emails from unknown senders in your inbox?	Rarely	1	
q20		a5	How often do you receive emails from unknown senders in your inbox?	Never	0	
q21		a1	Do you open emails from unknown senders?	Yes, all the time	4	
q21		a2	Do you open emails from unknown senders?	Most of the time	3	
q21		a3	Do you open emails from unknown senders?	Rarely	2	
q21		a4	Do you open emails from unknown senders?	Never	0	
q22		a1	What do you use your email account for? Note: Please only choose the primary purpose of your email account.	Professional	2	Depending on use, email address is divulgated to many individuals or few.
q22		a2	What do you use your email account for? Note: Please only choose the primary purpose of your email account.	Academic	1	
q22		a3	What do you use your email account for? Note: Please only choose the primary purpose of your email account.	Social	4	
q22		a4	What do you use your email account for? Note: Please only choose the primary purpose of your email account.	Shopping	3	
q22		a5	What do you use your email account for? Note: Please only choose the primary purpose of your email account.	Other (please specify)	other	Answer choices (Everything or personal) were rated 4.
q23		a1	Where do you open your email account? Choose all that apply.	University	1	Based on the place, probability is higher; the consequences of user's information being stolen vary accordingly.
q23		a2	Where do you open your email account? Choose all that apply.	Public Library	3	
q23		a3	Where do you open your email account? Choose all that apply.	Home	2	
q23		a4	Where do you open your email account? Choose all	Mobile Network	1	

			that apply.			
q23		a5	Where do you open your email account? Choose all that apply.	Public Network	4	
q23		a6	Where do you open your email account? Choose all that apply.	Other (please specify)	other	
q24		a1	What type of device do you use for accessing your email account? Choose all that apply.	Laptop	4	Most of users' information are usually on the device's storage. Laptop goes everywhere and usually has more space than tablet and cell.
q24		a2	What type of device do you use for accessing your email account? Choose all that apply.	Desktop	3	A desktop has a lot of storage must is not as portable.
q24		a3	What type of device do you use for accessing your email account? Choose all that apply.	Tablet	2	
q24		a4	What type of device do you use for accessing your email account? Choose all that apply.	Cell phone	1	
q25		a1	If you use campus desktops, do you have access to shared folders of other computers?	Yes	4	
q25		a2	If you use campus desktops, do you have access to shared folders of other computers?	No	0	
q25		a3	If you use campus desktops, do you have access to shared folders of other computers?	Not applicable	0	
q26		a1	If you use campus desktops, how many computers are accessed by sharing?	More than 18	4	
q26		a2	If you use campus desktops, how many computers are accessed by sharing?	12-17	3	
q26		a3	If you use campus desktops, how many computers are accessed by sharing?	6-11	2	
q26		a4	If you use campus desktops, how many computers are accessed by sharing?	Fewer than 5	1	
q26		a5	If you use campus desktops, how many computers are accessed by sharing?	Not applicable	0	

q27		a1	How do you use your email account? Choose all that apply.	Send email	2	
q27		a2	How do you use your email account? Choose all that apply.	Receive email	2	
q27		a3	How do you use your email account? Choose all that apply.	Shopping online	3	Include travel reservation.
q27		a4	How do you use your email account? Choose all that apply.	Social website	4	
q27		a5	How do you use your email account? Choose all that apply.	Other (please specify)	other	
q28		a1	How long have you had your email account?	More than 5 years	4	Heavy users have more spam and newer accounts receive less spam.
q28		a2	How long have you had your email account?	Between 3 but less than 5 years	3	
q28		a3	How long have you had your email account?	Between 1 but less 3years	2	
q28		a4	How long have you had your email account?	Less than a year	1	
q29		Skipped	Comments?		Skipped	
part2_part2 - q1	part2-q1	Skipped	Do you own a device with online email access? Note: If you have many devices, please only choose the one you use the most and/or daily.		Skipped	
part2_q2	q2	a1	Do you update your device against vulnerabilities?	Yes	0	
part2_q2	q2	a2	Do you update your device against vulnerabilities?	No	4	
part2_q3	q3	a1	How often do you update your device against vulnerabilities?	Monthly	2	Include as recommended or whenever prompted.
part2_q3	q3	a2	How often do you update your device against vulnerabilities?	Weekly	1	Include 3times/week or daily.
part2_q3	q3	a3	How often do you update your device against vulnerabilities?	Rarely	3	
part2_q3	q3	a4	How often do you update your device against vulnerabilities?	Never	4	
part2_q	q3	a5	How often do you update your device against	Other	other	

3			vulnerabilities?			
part 2_q4	q4	a1	Do you use a storage media? Choose all that apply.	External hard drive	4	External hard drive can hold more data. Includes cloud storage and dropbox.
part 2_q4	q4	a2	Do you use a storage media? Choose all that apply.	USB	3	USB are more popular.
part 2_q4	q4	a3	Do you use a storage media? Choose all that apply.	SD	2	SD, CD, DVD are equally usable.
part 2_q4	q4	a4	Do you use a storage media? Choose all that apply.	CD	2	
part 2_q4	q4	a5	Do you use a storage media? Choose all that apply.	DVD	2	
part 2_q4	q4	a6	Do you use a storage media? Choose all that apply.	Other	other	Not applicable was rated 0.
part 2_q5	q5	a1	Do you run an antivirus on your personal computer?	Yes	0	
part 2_q5	q5	a2	Do you run an antivirus on your personal computer?	No	4	
part 2_q5	q5	a3	Do you run an antivirus on your personal computer?	Don't have a personal computer	0	
part 2_q6	q6	a1	Do you run anti-spyware on your personal computer?	Yes	0	
part 2_q6	q6	a2	Do you run anti-spyware on your personal computer?	No	4	
part 2_q6	q6	a3	Do you run anti-spyware on your personal computer?	Don't have a personal computer	0	
part 2_q7	q7	Skipped	Please rate your provider email account versus your university email account if applicable.		Skipped	
part 2_q8	q8	a1	What is a good password length? Remember: A length includes letters, numbers and characters. A character is anything that is not a letter or a number.	More than 16	1	
part 2_q8	q8	a2	What is a good password length? Remember: A length includes letters, numbers and characters. A character is anything that is not a letter or	9-15	2	

			a number.			
part2_q8	q8	a3	What is a good password length? Remember: A length includes letters, numbers and characters. A character is anything that is not a letter or a number.	5-8	3	
part2_q8	q8	a4	What is a good password length? Remember: A length includes letters, numbers and characters. A character is anything that is not a letter or a number.	Fewer than 4	4	
part2_q9	q9	a1	What is a good password complexity? Remember: A character is anything that is not a letter or a number.	Letter, numbers and characters	1	
part2_q9	q9	a2	What is a good password complexity? Remember: A character is anything that is not a letter or a number.	Letters and number/letters and characters/numbers and characters	2	
part2_q9	q9	a3	What is a good password complexity? Remember: A character is anything that is not a letter or a number.	Letters Only/numbers only/ characters only	4	
part2_q10	q10	Skipped	Please rate the strength of the following security questions.		Skipped	
part2_q11	q11	a1	What do you do online? Choose all that apply.	Download	4	
part2_q11	q11	a2	What do you do online? Choose all that apply.	Send and receive e-mails	3	
part2_q11	q11	a3	What do you do online? Choose all that apply.	Chat	2	
part2_q11	q11	a4	What do you do online? Choose all that apply.	Read newspapers and articles	1	
part2_q11	q11	a5	What do you do online? Choose all that apply.	Research	1	
part2_q11	q11	a6	What do you do online? Choose all that apply.	Shop	2	
part2_q11	q11	Other	What do you do online? Choose all that apply.	Other	Other	

part 2_q12	q12	a1	How many different websites do you visit per day?	More than 18	4	
part 2_q12	q12	a2	How many different websites do you visit per day?	12-17	3	
part 2_q12	q12	a3	How many different websites do you visit per day?	6-11	2	
part 2_q12	q12	a4	How many different websites do you visit per day?	Fewer than 5	1	
part 2_q13	q13	a1	What type of website do you visit? Choose all that apply.	Social	4	
part 2_q13	q13	a2	What type of website do you visit? Choose all that apply.	Research	1	
part 2_q13	q13	a3	What type of website do you visit? Choose all that apply.	Music	3	
part 2_q13	q13	a4	What type of website do you visit? Choose all that apply.	News	2	
part 2_q13	q13	a5	What type of website do you visit? Choose all that apply.	Other	other	
part 2_q14	q14	a1	How many files do you download per day?	More than 12	4	
part 2_q14	q14	a2	How many files do you download per day?	8-11	3	
part 2_q14	q14	a3	How many files do you download per day?	4-7	2	
part 2_q14	q14	a4	How many files do you download per day?	Fewer than 3	1	
part 2_q15	q15	a1	What type of files do you download? Choose all that apply.	Executable	4	
part 2_q15	q15	a2	What type of files do you download? Choose all that apply.	Scripts	3	Include music.
part 2_q15	q15	a3	What type of files do you download? Choose all that apply.	Documents	1	
part 2_q15	q15	a4	What type of files do you download? Choose all that apply.	Photos	2	Photos are larger in size than documents and more people access them; plus there are usually transferred from

						some other equipment.
part 2_q 15	q15	a5	What type of files do you download? Choose all that apply.	Other	other	
part 2_q 16	q16	Skip ped	How many email accounts do you currently use?		Skip ped	
part 2_q 17	q17	Skip ped	Please choose a category which applies to you.		Skip ped	
part 2_q 18	q18	a1	Please rate your Internet experience level.	Heavy user	4	
part 2_q 18	q18	a2	Please rate your Internet experience level.	Above average	3	
part 2_q 18	q18	a3	Please rate your Internet experience level.	Average	2	
part 2_q 18	q18	a4	Please rate your Internet experience level.	Some	1	
part 2_q 19	q19	Skip ped	What is your gender		Skip ped	

Appendix B

Yahoo Sign up Questions

1st Question Set

-Select One-

1. What is the first name of your favorite uncle?
2. Where did you meet your spouse?
3. What is your oldest cousin's name?
4. What is your youngest child's nickname?
5. What is your oldest child's nickname?
6. What is the first name of your oldest niece?
7. What is the first name of your oldest nephew?
8. What is the first name of your favorite aunt?
9. Where did you spend your honeymoon?
10. -Type your question here-

2nd Question Set

-Select One-

1. Where did you spend your childhood summers?
2. What was the last name of your favorite teacher?
3. What was the last name of your best childhood friend?
4. What was your favorite food as a child?
5. What was the last name of your first boss?
6. What is the name of the hospital where you were born?
7. What is your main frequent flyer number?

8. What is the name of the street on which you grew up?

9. What is the name of your favorite sports team?

10. What is your first pet’s name?

11. What is the last name of your best man at your wedding?

12. What is the last name of your maid of honor at your wedding?

13. What is the name of your favorite book?

14. What is the last name of your favorite musician?

15. Who is your all-time favorite movie character?

16. What was the make of your first car?

17. What was the make of your first motorcycle?

18. Who is your favorite author?

19. -Type your question here-

AOL Sign up Questions

1st Alternative

Select a Security Question

1. What is your frequent flyer number?

2. What is your library card number?

3. In which city did your parents meet?

4. In what year was your mother born?

5. What was your favorite childhood cartoon?

6. What was your favorite childhood book?

7. In what year was your father born?

8. What was your childhood nickname?

2nd Alternative

Select a Security Question

1. What was your favorite childhood book?
2. In what year was your father born?
3. What was your childhood nickname?
4. What is your grandmother’s first name?
5. What is your father’s middle name?
6. In what city were you born?
7. What is your mother’s maiden name?
8. What was the name of your first pet?

Gmail Sign up Questions

Choose a Question

1. What is the name of your best friend from childhood?
2. What was the name of your first teacher?
3. What is the name of your manager at your first job?
4. What was your first phone number?
5. What is your vehicle registration number?
6. Write my own question

Hotmail Sign up Questions

Select One

1. Mother’s birthplace
2. Best childhood friend
3. Name of first pet
4. Favorite teacher
5. Favorite historical person
6. Grandfather’s occupation

GMX Sign up Questions

Choose One

1. What city were you born in?
2. What is your mother’s maiden name?
3. What was the name of your first pet?
4. Who is your favorite author?
5. What was the last name of your favorite teacher?
6. What is the name of the street on which you grew up?
7. What is the name of your favorite sports team?
8. Who is your all-time favorite movie character?
9. What was the make of your first car?

Glossary

If needed.

Bibliography

[1] AOL alternative sign up page. https://new.aol.com/productsweb/?promocode=827692&ncid=txtlnkuswebr00000073. [Online] Last accessed 10/23/2012.

[2] AOL sign up page. https://new.aol.com/productsweb/?promocode=825345&ncid=txtlnkuswebr00000106. [Online] Last accessed 10/23/2012.

[3] Cyber security news. http://cybersecuritynews.org/2012/06/29/hackers-take-a-hit-as-cybersecurity-industry-booms/#more-1954. [Online] Last accessed 06/10/2012.

[4] Federal times. http://www.federaltimes.com/section/IT01/Cybersecurity. [Online] Last accessed 06/10/2012.

[5] Gmail attachment information. http://support.google.com/mail/bin/answer.py?hl=en&answer=25760. [Online] Last accessed 10/23/2012.

[6] Gmail sign up page. https://accounts.google.com/SignUp?service=mail&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&ltmpl=default. [Online] Last accessed 10/23/2012.

[7] Homeland security news wire. http://www.homelandsecuritynewswire.com/dr20120912-civilian-cyberwarriors-not-motivated-by-patriotism. [Online] Last accessed 06/10/2012.

[8] Hotmail sign up page. https://signup.live.com/signup.aspx?wa=wsignin1.0&rpsnv=11&ct=1351022015&rver=6.1.6206.0&wp=MBI&wreply=http%3a%2f%2fmail.live.com%2fdefault.aspx%3frru%3dinbox&id=64855&cbcxt=mai&snsc=1&bk=1351022015&uiflavor=web&mkt=EN-US&lc=1033&lic=1. [Online] Last accessed 10/23/2012.

[9] Security awareness. http://www.securityawareness.com/secnews.htm. [Online] Last accessed 06/10/2012.

[10] Top ten reviews. http://free-email-services-review.toptenreviews.com/. [Online] Last accessed 10/23/2012.

[11] Yahoo sign up page. https://edit.yahoo.com/registration?.intl=us&.lang=en-US&.pd=fpctx_ver%253D0%2526c%253D%2526ivt%253D%2526sg%253D&new=1&.done=http%3A//www.yahoo.com/&.src=fpctx&.v=0&.u=al6glnd88dcoi&partner=&.partner=&pkg=&stepid=&.p=&promo=&.last=. [Online] Last accessed 10/23/2012.

[12] Adrian Fernandez, Emilio Insfran and Silvia Abrahão. Usability evaluation methods for the web: A systematic mapping study. *Information and Software Technology*, 53(8), August 2011, pages 789-817.

[13] Andreas Holzinger. Usability engineering methods for software developers. *Communications of the ACM*, 48(1), January 2005, pages 71-74.

[14] Asil Oztekin, Alexander Nikov and Selim Zaim. UWIS: An assessment methodology for usability of web-based information systems. *Journal of Systems and Software*, 82(12), December 2009, pages 2038-2050.

[15] Asil Oztekin. A decision support system for usability evaluation of web-based information systems. *Expert Systems with Applications*, 38(3), March 2011, pages 2110-2118.

[16] Ben Shneiderman. Universal usability. *Communications of the ACM*, 43(5), May 2000, pages 84-91.

[17] Bilge Karabacak and Ibrahim Sogukpinar. ISRAM: information security risk analysis method. *Computers & Security*, 24(2), March 2005, pages 147-159.

[18] Carl Colwill. Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 14(4), November 2009, pages 186-196.

[19] Carlos Flavián, Miguel Guinalíu and Raquel Gurrea. The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management*, 43(1), January 2006, pages 1-14.

[20] Catherine S. Weir, Gary Douglas, Martin Carruthers and Mervyn Jack. User perceptions of security, convenience and usability for e-banking authentication tokens. *Computers & Security*, (28, 1–2), February–March 2009, pages 47-62.

[21] Catherine S. Weir, Gary Douglas, Tim Richardson and Mervyn Jack. Usable security: User preferences for authentication methods in e-Banking and the effects of experience. *Interacting with Computers*, (22, 3), May 2010, pages 153-164.

[22] Cheng Xiang-Yun; Wang Ying-Mei and Xu Zi-Ling. Risk Assessment of Human Error in Information Security. In *Proceedings of the 5th International Conference on Machine Learning and Cybernetics*, 13-16 August 2006, pages 3573-3578.

[23] Christian W Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop. Insider Threats in Cyber Security: Aspects of Insider Threats. *Advances in Information Security*, volume 49, Springer US, 2010, pages 1-15.

[24] D. Balfanz.; G. Durfee; D. K. Smetters and R. E. Grinter. In search of usable security: five lessons from the field. *Security & Privacy, IEEE*, 2(5), September-October 2004, pages 19-24.

[25] D. Ramsbrock; R. Berthier and M. Cukier. Profiling Attacker Behavior Following SSH Compromises. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 25-28 June 2007, pages119-124.

[26] Darren Davis, Fabian Monrose, and K. Michael Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th conference on USENIX Security Symposium, volume 13*, 11-11.

[27] Denis Trcek, Roman Trobec, Nikola Pavesic, and J. F. Tasic. Information systems security and human behaviour. *Behavior and Information Technology*, 26(2), March 2007, pages 113-118.

[28] Divakaran Liginlal, Inkook Sim and Lara Khansa. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3–4), May–June 2009, pages 215-228.

[29] E. Eugene Schultz. Research on usability in information security. *Computer Fraud & Security*, issue 6, June 2007, pages 8-10.

[30] E. Eugene Schultz, Robert W Proctor, Mei-Ching Lien and Gavriel Salvendy. Usability and Security: An Appraisal of Usability Issues in Information Security Methods. *Computers & Security*, 20(7), 31 October 2001, pages 620-634.

[31] E. Jonsson and T. Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, 23(4), Apr 1997, pages 235-245.

[32] Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4), June 2007, pages 276-289.

[33] Eric D. Shaw. The role of behavioral research and profiling in malicious cyber insider investigations. *Digital Investigation*, 3(1), March 2006, pages 20-31.

[34] Erlend Bønes, Per Hasvold, Eva Henriksen and Thomas Strandenæs. Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International Journal of Medical Informatics*, 76(9), September 2007, pages 677-687.

[35] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems. Nist special publication 800(30), NIST, 2002, pages 800-30.

[36] Ghi Paul Im and Richard L. Baskerville. A longitudinal study of information system threat categories: the enduring problem of human error. *The Database for Advances in Information Systems,* 36(4), ACM SIGMIS, October 2005, pages 68-79.

[37] Gimun Kim, Bongsik Shin and Ho Geun Lee. A study of factors that affect user intentions toward email service switching. *Information & Management*, 43(7), October 2006, pages 884-893.

[38] Godwin J. Udo, Kallol K. Bagchi and Peeter J. Kirs. An assessment of customers' e-service quality perception, satisfaction and intention. *International Journal of Information Management*, 30(6), December 2010, pages 481-492.

[39] Gregg Vanderheiden. Fundamental principles and priority setting for universal usability. In *Proceedings of the Conference on Universal Usability*, ACM, 2000, pages 32-37.

[40] Gurvirender P.S. Tejay and Sean M. Zadig. Investigating the Effectiveness of IS Security Countermeasures towards Cyber Attacker Deterrence. *45th Hawaii International Conference on System Sciences*, 2012, pages 3051-3060.

[41] H. Lacohee, A.D. Phippen and S.M. Furnell. Risk and restitution: Assessing how users establish online trust. *Computers Security*, 25(7), October 2006, pages 486-493.

[42] Harry Hochheiser and Ben Shneiderman. Universal usability statements: Marking the trail for all users. *Interactions*, 8(2), ACM, March 2001, pages 16-18.

[43] Hock-Hai Teo, Lih-Bin Oh, Chunhui Liu and Kwok-Kee Wei. An empirical study of the effects of interactivity on web user attitude. *International Journal of Human-Computer Studies*, 58(3), March 2003, pages 281-305.

[44] Ignacio J. Martinez-Moyano, Stephen H. Conrad and David F. Andersen. Modeling behavioral considerations related to information security. *Computers & Security*, 30(6–7), September–October 2011, pages 397-409.

[45] Igor Nai Fovino, Marcelo Masera and Alessio De Cian. Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety*, 94(9), September 2009, pages 1394-1402.

[46] J. Johnston, J. H. P. Eloff and L. Labuschagne. Security and human computer interfaces, *Computers & Security*, 22(8), December 2003, pages 675-684.

[47] Jill Sweeney and Joffre Swait. The effects of brand credibility on customer loyalty. *Journal of Retailing and Consumer Services*, 15(3), May 2008, pages 179-193.

[48] Jose Torres, Jose Sarriegi, Javier Santos and Nicolás Serrano. Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. *Information Security,* volume 4176, Springer Berlin / Heidelberg 2006, pages 530-545.

[49] Julie Thorpe and Van P.C. Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, article 8, 2007, 16 pages.

[50] Julio Abascal and Colette Nicolle. 2005. Moving towards inclusive design guidelines for socially and ethically aware HCI. *Interacting with Computers*, 17(5), September 2005, pages 484–505.

[51] Kim-Phuong L. Vu, Vanessa Chambers, Beth Creekmur, Dongbin Cho and Robert W. Proctor. Influence of the Privacy Bird® user agent on user trust of different web sites. *Computers in Industry*, 61(4), May 2010, pages 311-317.

[52] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, article 1, 2008, 15 pages.

[53] M. Asif Khan and Mureed Hussain. Cyber security quantification model. *In Proceedings of the 3rd international conference on Security of information and networks*, ACM, 2010, pages 142-148.

[54] M. Roy, O. Dewitt and B. Aubert. The impact of interface usability on trust in web retailers. *Internet Research* [Online]. January 1, 2001; 11(5):388-98, ERIC, Ipswich, MA. Accessed September 27, 2012.

[55] Mark Keith, Benjamin Shao and Paul John Steinbart. The usability of passphrases for authentication: An empirical field study. International *Journal of Human-Computer Studies*, 65(1), January 2007, pages 17-28.

[56] Martin Fassnacht and Ibrahim Köse. Consequences of Web-based service quality: Uncovering a multi-faceted chain of effects. *Journal of Interactive Marketing*, 21(3), 2007, pages 35-54.

[57] Michael W. Boyce, Katherine Muse Duma, Lawrence J. Hettinger, Thomas B. Malone, Darren P. Wilson, and Janae Lockett-Reynolds. Human Performance in Cybersecurity: A Research Agenda. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, issue 55, September 2011, pages 1115-1119.

[58] Mikko T. Siponen and Harri Oinas-Kukkonen. 2007. A review of information security issues and respective research contributions. *The Database for Advances in Information Systems*, 38(1), ACM *SIGMIS*, February 2007, pages 60-80.

[59] N. Z. Khidzir; A. Mohamed and N. H. Arshad. Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. *International Conference on Information Retrieval & Knowledge Management*, 17-18 March 2010, pages194-199.

[60] Nancie Gunson, Diarmid Marshall, Hazel Morton and Mervyn Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4), June 2011, pages 208-220.

[61] P.A.S. Ralston, J.H. Graham and J.L. Hieb. Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, 46(4), October 2007, pages 583-594.

[62] R. Dantu; K. Loper and P. Kolan. Risk management using behavior based attack graphs. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, 1(5-7), April 2004, pages 445- 449.

[63] Rahul Telang and Tridas Mukhopadhyay. Drivers of Web portal use. *Electronic Commerce Research and Applications,* 4(1), July 2005, pages 49-65.

[64] Ramón Hervás and José Bravo. Towards the ubiquitous visualization: Adaptive user-interfaces based on the Semantic Web. *Interacting with Computers*, 23(1), January 2011, pages 40-56.

[65] Roy A. Maxion and Robert W. Reeder. 2005. Improving user-interface dependability through mitigation of human error. *International ournal of. Human-Computer Studies*, 63(1-2), July 2005, pages 25-50.

[66] Rui Lopes and Luís Carriço. The impact of accessibility assessment in macro scale universal usability studies of the web. In *Proceedings of the 2008 international cross-disciplinary conference on Web accessibility,* ACM, 2008, pages 5-14.

[67] S. Colombo and M. Demichela. The systematic integration of human factors into safety analyses: An integrated engineering approach. *Reliability Engineering & System Safety*, 93(12), December 2008, pages 1911-1921.

[68] Sara Kraemer and Pascale Carayon. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), March 2007, pages 143-154.

[69] Sara Kraemer, Pascale Carayon and John Clem. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), October 2009, pages 509-520.

[70] Sebastian Möller, Noam Ben-Asher, Klaus-Peter Engelbrecht, Roman Englert and Joachim Meyer. Modeling the behavior of users who are confronted with security mechanisms. *Computers & Security*, 30(4), June 2011, pages 242-256.

[71] Shareeful Islam and Wei Dong. Human factors in software security risk management. In *Proceedings of the first international workshop on Leadership and management in software architecture*, ACM, 2008, pages 13-16.

[72] Shari Lawrence Pfleeger and Deanna D. Caputo. Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, 31(4), June 2012, pages 597–611.

[73] Simon E. Parkin, Aad van Moorsel, and Robert Coles. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2nd International Conference on Security of Information and Networks*, ACM, 2009, pages 46-55.

[74] T. Sommestad; M. Ekstedt and P. Johnson. Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Model. *42nd Hawaii International Conference on System Sciences*, 5-8 Jan 2009, pages 1-10.

[75] Toni Perković, Shujun Li, Asma Mumtaz, Syed Ali Khayam, Yousra Javed, and Mario Čagalj. Breaking undercover: exploiting design flaws and non uniform human behavior. In *Proceedings of the Seventh Symposium on Usable Privacy and Security,* ACM, article 5, 2011, 15 pages.

[76] Volker Roth, Tobias Straub, and Kai Richter. Security and usability engineering with particular attention to electronic mail. *International Journal of Human-Computer Studies*, 63(1-2), July 2005, pages 51-73.

[77] W. Saad; T. Alpcan and T. Basar; A. Hjorungnes. Coalitional Game Theory for Security Risk Management. *Fifth International Conference on Internet Monitoring and Protection*, 9-15 May 2010, pages 35-40.

[78] William B. Askren, Thaddeus L. Requlinski. Quantifying Human Performance Reliability, *Air Force Human Resources Lab*oratory, Wright Patterson AFB, Ohio Advanced Systems Div., AFHRL-TR-71-22, June 71, 17pages.

[79] Yasuko Kanno, Masato Terada, Hidehiro Yajima, Toshinari Kamamura, and Norihisa Doi. A comparative study on structure of the motivation for information security by security incident experiences. In *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*. ACM, 2009, pages 9-16.

[80] Ye Diana Wang and Henry H. Emurian. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), January 2005, pages 105-125.