International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.85-96
http://dx.doi.org/10.14257/ijsia.2014.8.5.09

Usability Analysis on Security of E-mail Accounts: Differences between Fantasy and Reality

Zara Tariq [1] and Ramsha Arif[2]

Jinnah University for Women, Karachi, Pakistan
[1]zara.tariq_cs@yahoo.com, [2]email2ramsha@yahoo.com

Abstract

As this era is known as Electronic era where everything is associated with Internet and its growing number of security threats. In our study, we focused on three different e-mail account securities, comparatively. First, by performing an analysis on online E-mail service providers we concluded that what type of functionalities they are providing to secure their user's information. Second, we categorized users in to three types and on the basis of that we study on user's view on online security, confidence and usability on their E-mail service provider. Third, we evaluate the outcome of our study which emphasizes the user's precautions from protecting their accounts from unauthorized access. The goal is to analyze how users perceive the security of their email account based on the domain in which it was created. 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 and business users. The reality analysis will allow us to examine and possibly classify the email providers based on their security parameters and users account protection levels. 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.

Keywords: *Google mail, MSN mail and Yahoo Mail, Account's security, Usability, Perception*

1. Introduction

The security of virtual data is experiencing high risks these days as the number of its users growing. Although all security providers are working strenuously in introducing indestructible security but simultaneously people are destructing their security by hacking or the utmost competition in market makes their security systems weak.

Nowadays, the main challenge is to protect the user's personal and sensitive data on user's e-mail accounts which is always a big dispute. As the utility of free of charge web mails is very common and it can be access anywhere. Only web browser and internet connection is required. In the meantime, e-mail service providers give their users huge capacity to fulfill their need of storing large data. P.S. they provide a cloud for their user to access mobile data.

Our research study is to contrast the three famous E-mail service providers which are Google mail, MSN mail and Yahoo Mail.

Relating on study [3], proposed a theory for risk revealing which considers judgment, learning theories and decision-making. Human flaws can proceed to susceptibilities.

Similarly a vast research [10, 2] which is based on the role of human flaws in security threats. Both theories organize the threats in two main primarily contradictory classes: deliberate and accidental. We appraise the applicable research on usability, human computer

ISSN: 1738-9976 IJSIA

interaction, and security of information, user's expectation, online web-based systems, protected communication and user opinion. We express an observation in which user's opinion is examined in means of authentication and security causes.

The motive of this research is an effort to implement some easy and reliable techniques on information security systems [11]. By performing a comparison based on efficiency and security, the approach is to begin by analyzing unlike free of charge E-mail service providers. Then will pursue the study analysis on E-mail account's security as observed by some professional and the students of Jinnah University for Women. On the security constraints and users account security levels, the certain analysis will let to observe and probably sort the E-mail providers.

2. Purpose and Motivations of the Study

The aim of this project was to evaluate the usability of three most popular E-mail Accounts: Google mail, MSN mail and Yahoo Mail, in respect of security and safety [4]. This sector was chosen due to the fact that the convenience of web-based e-mail services is unrivaled, where all your mail is stored in one central location and remains easily accessible from any computer on the internet. Also, the limited amount of research on evaluation methods was a major incentive for the project.

3. Aims of the Study

1. To evaluate how usable and easily accessible security of each site.
2. To measure the success rate, average task times, error [3] rate and user's expressions through alternatives usability evaluation methods in order to understand the user experience.
3. To observe what the usability are problems that make the functionalities fallow.
4. To identify the user's perception and importance of e-mail accounts in their point of view.
5. To examine which e-mail account is mostly used and what its reason.
6. To conclude which site has provided more usable security.

4. Method

The methods which were chosen for the evaluation of the web based e-mail accounts are: 1) Cognitive Walkthrough Method that helps the evaluator to come up with success or failure of the task based on the interface design and user's knowledge; 2) Usability questionnaire.

4.1. Study Design

The three levels we identified are the usage and recovery security: First level is user should follow the strong password rules while creating an account i.e. accounts security at the time of account creation. Second, on the basis of recovery security is very important. That means if you're going to recover your account how much usable it is and how securely you can recover it. Third, password session time-out and to change the password when account is login.

The moral of this study is user's account shouldn't be compromise as if anybody can easily recover his/her account. Also, implementing strong password doesn't mean account is safe until user has improvised the security of account.

The Dependent variables are time, no. of errors and emotions that are observed when user performing task and the independent variables are interface [14] of email accounts.

4.2. Participants

We categorized users into three groups Academic Users who regularly uses their E-mail account and like to explore all the features and try to use them to enhance their privacy and security, they are usually really well aware of the new features and updates which their E-mail service[12] provider provides them. Secondly, Professional Users who usually uses their E-mail accounts according to their job requisites and they are not concern to explore the features. They only know basic features or any feature that their work related. Thirdly, Personal Users who uses their E-mails casually and mostly they created their accounts for linking to social media and other sites which required user IDs for verifications and subscriptions most commonly like Facebook or Twitter account creation.

Total number of participant we used for our research are 40, out of which 5 were males and 35 were females users of E-mail accounts on the basis of academic, professional or personal users. Participants were from a Jinnah University for Women University and some other home users and ranged in age from 16-30 years old. Participants were chosen using a laptop or desktop computer on a daily basis or at least twice a week.

4.3 Materials

We have used Camtasia Studio [1], a tool for capturing screen audio and video. We used this tool as a measuring instrument of time, no. of errors and user's response. Moreover, this will also help us in task evaluation analysis. For the questionnaires, there is an online form which provides an efficient way to accomplish the questionnaires. There are two separate forms; one for survey questionnaire and another is for post-test questionnaire. Both tasks and questionnaires are presented in most attainable manner.

4.4. Procedure

Participants were explained that the purpose of the study was to determine and test the email accounts security in term of recovery of them if the passwords are missed or forgotten. They were elucidate that they have to assume as they has forgotten their password and have to recover their accounts just by using the ID or aliases they uses to logged-in. Choice of three E-mail Services providers were given (Google Mail, Yahoo Mail and MSN Mail).Users were given full freedom to independently choose which most frequent E-mail service they uses, they have to login and try to recover it by using any method of recovery they have set if they had forgotten their password.

Think aloud technique and co-operative environment were provided to the participants and were asked to perform their tasks loudly and if they do not understand or face any trouble while performing it they can ask for some help. After completion of task they have given feedback from comprise of questioner relating to the tasks and personal experience they gained throughout. For post evaluation we record screen with the users video to analyze the expressions of them and moreover time of completion of each task plus number of errors were also perceived to assess frequency of recovery presuming by different E-mail service providers. We also studied which E-mail service has the rapid and easy recovery process and which one is leading and famed for their usage regarding to account security and provide totally secure access to their authenticated users. After all study we determine comparatively among all three E-mail service provider which one gives its users the most secure services in addition to great performance simultaneously without compromising of effectiveness and efficiency.

Firstly, user required to proceed to their recovery procedure by entering their ID or aliases they needed to choose recovery method they have setup such as alternate E-mail, 2-step

verification or security question and after completion of recovery if they do not know about two step verification, we guide them all about it and help them to setup it to make them accounts more secure and accessed by only authenticated user.

4.5. Tasks

Task 1. Login your account, assuming that you have lost your password/user name: In this task we asked the users to login their E-mail accounts and assume that they do not remember their passwords and now try to recover it by whatever method of recovery they have chosen we studied that which recovery method did the user setup in case if he/she forgotten his password

Task 2. Setup High level (2-step verification) security on your email account: After completion of task one the users were promoted to this task in which we guide them and tell them the brief information about how account security is directly connected to High Level of security method like 2-Step Verification which is enforced by almost every E-mail service provider, for setting-up this technique you just required your mobile phone with you and after enabling this powerful feature your account could be completely secure by all unauthorized access.

We also studied that which E-mail provider gives easy recovery method and which one is more complex and have highly unbreakable processes to get recovery or access by any 3rd person for illegal purpose.

5. Results

In results section, we are discussing the summary of all study concisely for user experience, and their knowledge about security in terms of their E-mail accounts and unauthorized access possibility rate, their perceptions on what E-mail account provider is leading in market for its security, efficiency and performance rate and what it is in reality. The effort in whole research is extracted here in graphical representation which elevates the transparent outcome of our work.

The task was performed by two different groups. One group is of students of Jinnah University for Women who will perform tasks and answer the post-test questionnaire and second group is concerned about those who uses E-mail accounts on daily, twice a week or for some other purposes.

The following graphs show the frequency of user's performance while executing task on three different E-mail accounts. The Google mail is fastest among all three in executing tasks. The highest peak of Yahoo mail shows that it's more time-consuming while MSN mail has an average time-rate.

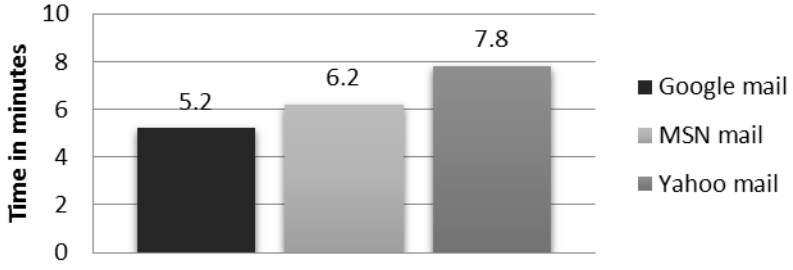

Figure A. Time Taken by Participant to Complete the Task

Considering the error frequency on number of participants, MSN mail gives minimal error rate. Google mail is also on side by side with MSN mail while Yahoo mail gives the highest error rate which shows its erroneous usability.

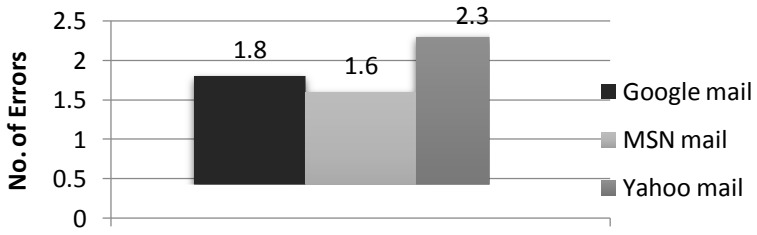

Figure B. Number Errors Done by Participants While Performing Tasks

5.1 Analysis and Discussion

To substantiate our objectives, we went through the users of all three E-mail service providers to validate our hypothesis and by those estimations we could achieve our goal which was to know that what E-mail service provider is leading successfully in the path of providing security to its users. We had total of 8 hypotheses which are further preceded by some of the discussion.

5.1.1 Hypothesis

1. People don't care that their account could be compromised.
2. People don't consider themselves responsible for the misuse of their passwords.
3. People use same passwords for their different accounts.
4. People are not aware of 2-Step Verification.
5. Setting high security, sometimes lacking the usability.
6. People get annoyed of spammed ads/mail.
7. Yahoo mail provides better services than Google mail and MSN mail.
8. People are really concern about their data security as they have all type of personal and official information on their account but don't explore the privacy and security polices of their accounts.

To justify our hypothesis, we are going to briefly delineate the arguments that are the causes of our hypothesis with paying keen attention to the type of users (*i.e.*, academic, personal, professional users).

Argument 1: People don't care that their account could be compromised.

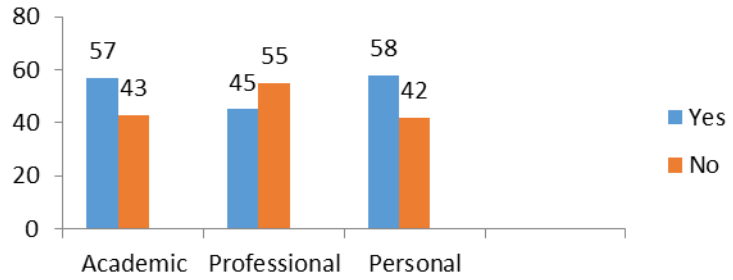

Figure C. Users Maintain Separate E-mail Accounts for Personal and Official Purposes

We thought that the majority of people of any group do not care about their E-mail accounts and they even don't know that their account could be compromised if they don't pay attention to their secure their accounts, as every user have many type of documents, pictures, videos and confidential information.

To evaluate this hypothesis, we asked to our all participant whether they are concern about their account or not. We concluded that majority of academic users created a separate accounts for their personal and academic use and the reason was they do not trust their school network or the environment where they login, the results says that they are afraid of hacking and unauthorized access of their personal interests. Throughout study says 55% people created separated E-mail accounts for their personal information and work based information.

Argument 2: People don't consider themselves responsible for the misuse of their passwords.

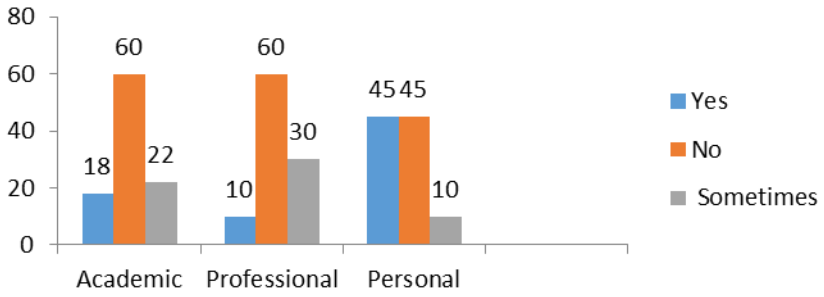

Figure D. Users Share their Passwords with Others

In this argument, we examined that some people share their passwords and they do not aware of the fact that their accounts could be hacked or misused [6]. We personally observed that most of the people setup their passwords which are easy for them to remember. They don't realize if they do so their account's security could be compromised. 32.9% of users set easily passwords throughout and results also proved that 57.3% people don't change their passwords for any reason within six months.

Argument 3: People use same passwords for their different accounts.

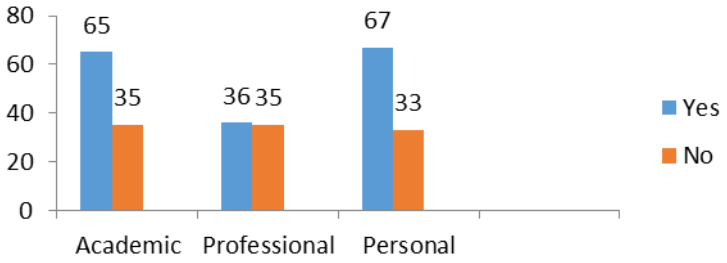

Figure E. Users Uses Same Passwords for their Different Accounts

In this arguments we have this theory that people uses same passwords and their perceptions for multiple accounts just to make their selves remember it [7]. This act of the users make the high rate of usability but no doubt on the same time they put their privacy and security in risk and which is directly proportional to jeopardy of their E-mail accounts and that may cause them to lose their information. For this we asked the participants as if they

uses same passwords [8] for different accounts and then about 60.97% of people said they does.

Argument 4: People are not aware of 2-Step Verification.

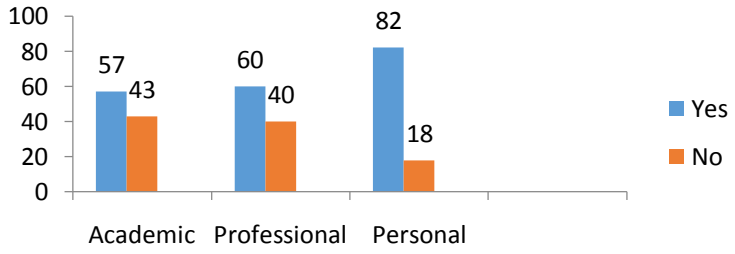

Figure F. Users Knows About 2-Step Verification

We presumed that majority of people don't know two step verification methods and just because of that their account's privacy and security might compromised. During the testing, we observed that 66.3% of users are known and 33.6% of users are not known to it although they want to know about it but they don't want to apply it. 32.6% gave reason that they don't feel safe giving their personal phone number to E-mail service providers. We notify benefits of this security while resetting their password but 53.6% users said they use alternate email approach and 39.6% use mobile code approach and those who approach security questions were negligible.

Argument 5: Setting high security, sometimes lacking the usability

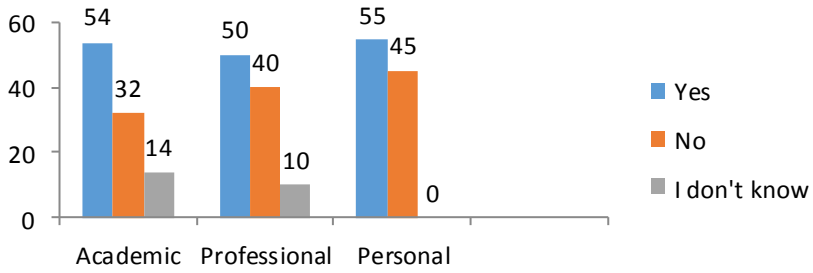

Figure G. Users Think it's Quite Hectic to Enter Code Every Yime

This hypothesis proves that when it comes to high security, there is always a trade-off of usability. More than 50% users find that setting high security becomes hectic as they have to enter the code comes to their mobile again and again to precede when using different E-mail service in public and specially when they use their account for daily purposes. When using E-mail service at their personal computers, 34% of users save their passwords for the sake of usability but 66% of users said that they don't feel safe because they think that their personal information may be compromised.

Argument 6: People get annoyed of spammed ads/mail

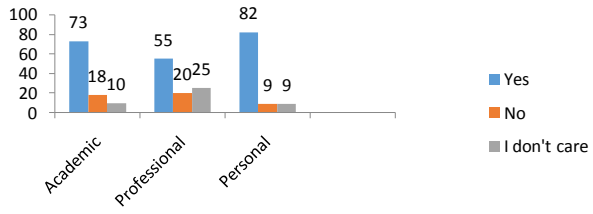

Figure H. People Get Annoyed of Spammed Ads/Mail

Although now E-mail service providers have worked a lot on spammed mails by filtering that actually disrupts user a lots but the climate of ads is still make users uncomfortable and this thing actually reflects on the usability of any service provider. Also E-mail service provider asks for money to remove ads. 70% of users are known the truth behind these spammed ads/mails, 27.3% of users feels safe clicking on them and 14.6% of users give a damn as they don't care about it.

Argument 7: Yahoo mail provides better services than Google mail and MSN mail

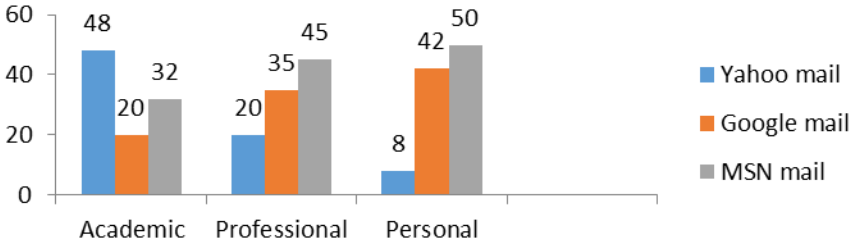

Figure I. E-mail Service Provider Best in Users Point of View

According to the study on the finest security provider, we found that Yahoo provides superior mail services in comparison with MSN and Google but while testing when we come to find this at end-user, we have found that our hypothesis actually contradict with our study as 25.3% of users voted for Yahoo, 32.3% of users voted for Google and at the same time 42.3% of users said that MSN is the best mail service provider which ensures that users are not aware of back-end security or they never investigate the security provided by different E-mail service providers.

Argument 8: People are really concern about their data security as they have all type of personal and official information on their account but don't explore the privacy and security polices of their accounts.

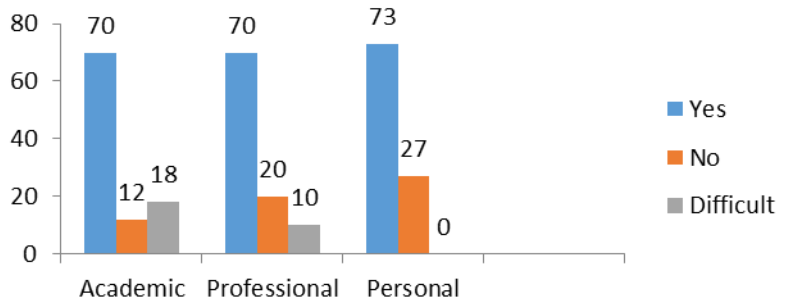

Figure J. Users Never Explore their Email Account's Privacy and Security Settings

Users have all types of data on their accounts such as personal data like photos, videos, and many more similarly their official and confidential stuff on it. People [5] always needed high security to protect their belongings but they still don't explore the enhanced features that their E-mail service providers facilitate them with. This is due to 20% of users don't feel it important and on the other hand 51% of people blindly trust their service providers and the level of trust is that much high, they don't know their E-mail service provider could even open the mails they have or they own [9].

TABLE 1. Table of Hypothesis

No.	Hypothesis	Survey Question	Responses (Academic Users)	Responses (Personal Users)	Responses (Professional Users)
1.	People don't care that their account could be compromised.	Do you maintain separate E-mail accounts for personal and official purposes	Yes=58% No=42%	Yes=45% No=55%	Yes=55% No=45%
2.	People don't consider themselves responsible for the misuse of their passwords.	Do you share your password with anyone	Yes= 18% No= 60% Sometimes= 22%	Yes= 10% No= 60% Sometimes= 30%	Yes= 45% No= 45% Sometimes = 10%
		Do you ever thought your accounts could be hack	Yes= 20% No= 14% May be= 33%	Yes= 15% No= 20% May be= 65%	Yes= 27% No= 45% May be= 27%
		Do you change your passwords (at least) within 6 months	Yes=28% No=48% For reason (*e.g.*, hacked/ stolen)=24%	Yes=29% No=62% For reason (*e.g.*, hacked/ stolen)=10%	Yes=23% No=54% For reason (*e.g.*, hacked/ stolen)=23

					%
		Do you follow the rules for creating your passwords	Yes= 76% No, I make it as easy as I could remember= 24%	Yes= 65% No, I make it as easy as I could remember= 35%	Yes= 65% No, I make it as easy as I could remember= 35%
3.	People use same passwords for their different accounts.	Do you use same passwords for different ID's	Yes, sometimes=65% No, always different=35%	Yes, sometimes= 65% No, always different=35 %	Yes, sometimes =67% No, always different=3 3%
4.	People are not aware of "2-Step Verification".	Do you know about 2-Step Verification?	Yes=57% No=43%	Yes=60% No=40%	Yes=82% No=18%
		Do you feel save giving your personal number for validation of your e-mail accounts	Its Safe=35% Not safe=65%	Its Safe=73% Not safe=27%	Its Safe=21% Not safe=79%
		In what way you reset your password if you forgot	Mobile= 16% Alternate E-mail account=64% Security question=20%	Mobile= 30% Alternate E-mail account=70 % Security question=0 %	Mobile= 73% Alternate E-mail account=27 % Security question=0 %
5.	Setting high security, sometimes lacking the usability	Do you think it's quite hectic to enter code every time	Yes=54% No=32% I don't know=14%	Yes=50% No=40% I don't know=10%	Yes=55% No=45% I don't know=0%
		Do you save your ID and password to your browsers of your personal computers	Yes=34% No, I don't feel secure= 66%	Yes=34% No, I don't feel secure= 66%	Yes=34% No, I don't feel secure= 66%
6.	People get annoyed of spammed ads/mail.	Do you know about SPAM emails that they are harmful for your personal data	Yes=73% No, they are okay=18%	Yes=55% No, they are okay=20%	Yes=82% No, they are okay=9%

			I don't care=10%	I don't care=25%	I don't care=9%
7.	Yahoo mail provides better services than Google mail and MSN mail.	Which E-mail services do you use?	Yahoo mail=48% Google mail=20% MSN mail=32%	Yahoo mail=20% Google mail=35% MSN mail=45%	Yahoo mail=8% Google mail=42% MSN mail=50%
8.	People are really concern about their data security as they have all type of personal and official information on their account but don't explore the privacy and security polices of their accounts.	Do you ever explore your email account's privacy and security settings	Yes=70% No not important=12% Difficult to understand=18%	Yes=70% No not important=20% Difficult to understand=10%	Yes=73% No not important=27% Difficult to understand=0%
		Do you open your Spam/Junk E-mails	Yes= 28% No= 72%	Yes= 40% No= 60%	Yes= 45% No= 55%
		Do you blindly trust your E-mail service provider that will secure your information?	Yes, off course= 52% No, not that much= 48%	Yes, off course= 55% No, not that much= 45%	Yes, off course= 45% No, not that much= 55%

6. Conclusion

The upcoming future of E-mail accounts is questionable until the atmosphere of online trust is build and the loopholes filled with the fulfillment of user's expectation. In this research, we observed that the interface is actually plays a big role in inducing trust on user's perception. To make the benefits of provided security we still need an educated user who has all the knowledge about the security risks and threats that are dangerous for user's account. So, for this user should also learn in what ways he can protect his account. The levels to authenticate security discussed are very important to protect data. Studies based on (1, 2 and 5) arguments, revealed that users all required is usability, however they know that there choice of convenience make their security on risk. User foresees a fast and trustable name of E-mail provider that's why they don't consider setting high security because there perception is that they have to wait for a long time[13]. Summing up the whole research analysis, that the more favorable and usable E-mail service providers are Google and MSN. However, the outcome declares that MSN is probably more adopt by users. The reason of 38% users prefers MSN mail because of its efficient, simple and smooth interface. Our research marked that users' perception is always that there account is at less risk but this is against the reality.

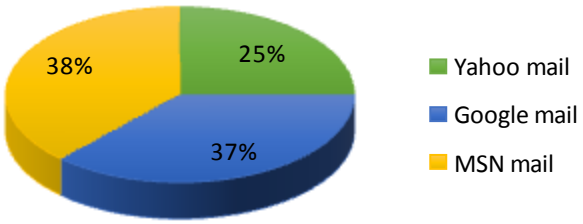

Figure K. Outcome of Usability Analysis

References

[1] "Camtasia Studio – Wikipedia", Retrieved from Wikipedia, **(2014)** January 1, http://en.wikipedia.org/wiki/Camtasia_Studio
[2] G. P. Baskerville, "A longitudinal study of information system threat categories: the enduring problem of human error", The Database for Advances in Information Systems, ACM SIGMIS, **(2005)** October, pp. 68-79.
[3] S. K. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists". Applied Ergonomics, vol. 38, no. 2, **(2007)** March, pp. 143-154.
[4] T. Chomsiri, "A Comparative Study of Security Level of Hotmail, Gmail and Yahoo mail by using session hijacking test", IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 5. **(2008)** May.
[5] J. Zhou and W.-Y. Chin, "An Effective Multi-Layered Defense Framework against Spam", Institute for Infocomm Research.
[6] N. S. P. Dewan, "ChaMAILeon: Exploring the Usability of a Privacy Preserving Email Sharing System". Bibsonomy. **(2013).**
[7] J. H. Yang, "BIBLIOGRAPHY, Method for generating and managing a user account using a multi-password", **(2012)** November 2.
[8] G. N. Thomborson, "Passwords and perceptions", In Proceedings of the Seventh Australasian Conference on Information Security, vol. 98, **(2009)**.
[9] C. Flavián, M. Guinalíu and R. Gurrea, "The role played by perceived usability, satisfaction and consumer trust on website loyalty", Information & Management, vol. 43, no. 1, **(2006)** January, pp. 1-14.
[10] D. Trcek, R. Trobec, N. Pavesic and J. F. Tasic, "Information systems security and human behavior", Behavior and Information Technology, vol. 26, no. 2, **(2007)** March, pp. 113-118.
[11] E. Bønes, P. Hasvold, E. Henriksen and T. Strandenæs, "Risk analysis of information security in a mobile instant messaging and presence system for healthcare", International Journal of Medical Informatics, vol. 76, no. 9, **(2007)** September, pp. 677-687.
[12] G. Kim, B. Shin and H. G. Lee, "A study of factors that affect user intentions toward email service switching", Information & Management, vol. 43, no. 7, **(2006)** October, pp. 884-893.
[13] H. Lacohee, A. D. Phippen and S. M. Furnell, "Risk and restitution: Assessing how users establish online trust. Computers Security, vol. 25, no. 7, **(2006)** October, pp. 486-493.
[14] M. Roy, O. Dewitt and B. Aubert, "The impact of interface usability on trust in web retailers", Internet Research [Online], **(2001)** January 1, vol. 11, no. 5, pp. 388-98,
[15] ERIC, Ipswich, MA. Accessed, **(2012)** September 27, 2012.