The Impact of Frequent Use Email When Creating Account at the Websites on the Users Privacy and Security

Salwa Al-Samirrai[1], Zahra Fadhil Mohsen[2] and Aysh Alhroob[2]

[1]College of Administrative and Financial Sciences, Isra University, Amman, Jordan
[2]Faculty of Information Technology, Isra University, Amman, Jordan

ABSTRACT

This research aims to measure the impact of frequent use of emails when creating account at the websites on the privacy and security of the user (a survey study conducted on a sample of email users' views). The sample, 200 people of the Jordanian society, includes employees of commercial and communication companies, banks, university students, employees and faculty members as well as computer centers at universities. All have emails and are able to use the computer and internet. A questionnaire has been prepared for this purpose aims to measure the variables of the study. SPSS program was used to analyze the results. The study revealed the existence of a statistical significant impact of frequent use of email account when creating an account at the Internet sites on the security and privacy of the user. The study concluded a number of conclusions and recommendations.

KEYWORDS

e-mail, security, privacy, Internet sites, password, username.

1. INTRODUCTION

The development of applications relying on the internet and its multi services provided, make the users feel that they badly need to benefit of these services in their all areas of daily life; for example the services provided by Facebook, Twitter, Google and LinkedIn. Some people use Google for researching, translation services, while other sites serve the social communication; such as Facebook and Twitter, to encourage more individuals to join social activities. Many websites are called e-trade used to commercial transactions, sales and procurement, or shopping through internet, such as EBay and Amazon, which allow the engaged members to execute selling and purchasing transactions. Internet services created multi problems pertaining to the security and privacy of the users and how to keep them safety in the new open environment generated by the internet.

These problems had arisen out of the conditions to benefit of these services, which require the user to generate an account in the website, including (user name, postal address and password). The user may use the same information for multi registering in multi websites, which generates multi problems to the user in respect of his privacy and security.

Therefore, we can conclude from the foregoing that the recent developments in the area of the internet usage and its created broad space to provide various services to various categories users, has become risky.

DOI : 10.5121/ijcsit.2013.5601

Due to the novelty of users dealing with websites in the Arab countries, the users face a problem in dealing with the websites and how to maintain their main e-mail privacy and security. The most important difficulty rose through dealing with the use of the main e-mail address when registering in more than one websites or the use of the same name and password. The problem becomes complicated by picking simple password, for example, the use of birth year or the name of his child or any other easy-detected by hackers, or he did not read the conditions of privacy and use defined by the websites, assuming that the websites would protect his privacy or the conditions are written in English and he is not able to read and understand as his interest is to get access to the services provided by these websites.

The lack of interest in these matters may make it suffers from the problem of the infringement of his email address security and privacy, which may be represent the email of his employment institution, leading to endanger his work place privacy an security to be infringed as his email contains many private work emails messages. He may also be bothered by receiving many messages from unknown people which contain viruses. Users and many interested in this subject might think that the users are responsible for this problem, but in fact the designers also share liability because the design of the user's page may does not keep, technically, the privacy and security of the user data.

This survey conducted on a random sample of various websites users, who have email accounts, concluded that these people face such difficulties. The major reason behind these problems may be the lack of experience in privacy and security of this area. Therefore, the researchers will attempt in this research to detect the problems of privacy and security the internet websites users face by frequent use of their email address when registering in these websites, explore the reasons and set recommendations that guarantee the privacy and security of the users in their dealing with the various internet websites. The presentation of the concept, importance and security and privacy of e-mail addresses will be addressed as one of this research aims. Furthermore, Clarifies the basic requirements set by Internet websites from the user when creating an account therein to get benefit of its various services. This research analyzes the impact of repeated use of e-emails when registering in more than one website s on the security and privacy of the user.

The importance of this research arises in dealing with a new-generated subject covered by few researchers at world-wide level to the knowledge of the researchers, in addition to the scarcity of Arab studies in this area. The results and recommendations of this study may contribute to add scientific knowledge and draw the attention of researchers to be interested in such topics.

Hypotheses

On the basis of the problem, the following hypothesis can be formulated:

"There is no moral impactful relation of statistical significance at the level of ≤ (0.05) between the repeated use of email address by the user when registering at the different websites and the protection of his privacy and security".

The rest of the paper is organized as follows: Related work is presented in Section 2. Section 3 covers Approach of the research. Theoretical framework is covered in Section 4. Section 5 introduces the result discussion. The conclusion and future work recommendation are discussed in Section 6.

2. PREVIOUS WORKS

Edward W. Felten & Shieley Gaw Study in [1] introduced a use of the password in each correspondence on the Internet, subscription with services, and shopping accompanied by growing concern about the possibility of theft of email addresses as a result of repeated use of the same password in multiple accounts. This may weaken the password and potential of being hacked. The study was conducted on (49) undergraduate students who were questioned "how many passwords they have and how often they reuse them".

It was found that that the majority of users have three passwords or less. The passwords are used twice at least. They do not use new a password in each new account they sign up. This is wrong behaviour because users think their re-use of the same password would enable them to manage it. The users point out that threats emerge from close people and they used their phone numbers as a password. The study provides several recommendations relevant to the improvement the management of current password and the use of strong password.

A large-Scale Study of Web Password Habits by Dinei Florencio & Cormac Herley in [2], the authors addressed the negative effects resulting from the use of the password by the users. The Study includes half million user and lasted for three months, focusing on the mechanism of registration the password and the strength of the different passwords used by the user, as well as the measurement of these passwords. The study concluded to calculate or estimate the average number of passwords and the average number of accounts of each user and the extent of password participation in the user accounts, in addition to the number of times the user forgets the password, strength, length, and type of the password and its difference according to the websites.

The subject of the passwords was addressed in a study conducted in [3], the user-specific information and access to it is secured by a password, which has become one of the most important topics today. The users have become more interested than ever before in maintaining the security and privacy of the password. The establishment and management of the password has become of topics of vital importance. Therefore, certain policy for the password must be developed and applied. The study concentrated on identifying and modelling password policy and discussed the password policy being followed in its management. The study provided a simulation model, with a set of variables and algorithms, to simulate the password; in addition to several results to the password simulation.

A study in [4], conducted by the group of information security. The survey study was conducted on more than (1000) Internet users aged between 18 - 82 years old. It indicated that privacy is of deemed a major concern of internet users. The study concluded that (51.3 %) of the users do not trust the privacy policy declared by the websites and (28.5 %) only had answered the question positively when asked: Do you think that Websites would adhere to and meet the privacy policy they declare?

In [5], an important topic related to the wrong behaviour of the user when using his email, or sometimes called the user name, when registering in the websites, and subsequent problems relevant the security and privacy of the user. This was made through studying the design diagram of password recovery system used by the websites or the technology used to maintain the user privacy. The study concluded that the repeated use of email as ID faces many risks pertinent to the privacy and security of the user. There are difficulties facing the current solutions. The study suggested many solutions that can be used to protect the ID user on the internet and achieve better system management to the user ID in the future.

Through this rapid review to the conclusions of the previous studies, this study attempts to diagnose the problems the Arab users suffered in using the websites, their awareness of such problems and the impact of the frequent use of the email address on the user privacy and security.

3. APPROACH OF THE RESEARCH

The descriptive analytical approach has been adopted in the research, depending on the field method in collecting the data through the questionnaire, which has been statistically analyzed to the test the reliability of the hypotheses using Statistical packages (SPSS). Moreover, the researchers conducted personal interviews with some individuals of the sample, reviewed previous studies for the purpose of preparing the questionnaire. Desktop survey also took place through the references, scientific journals and websites to develop the theoretical framework of the research, beside exploration of the most important previous studies, which constitute a vital resource to the research and their content of core knowledge.

3.1 Community of the Search Sample

The research community consists of individuals of Jordanian society working in commercial companies, telecoms, banks and universities, including students, employees of computer centres and faculty members. The sample, 220 individuals, was randomly selected, represents those who have emails accounts that able to use the computer and internet. Table 1 shows the number of analyzable questionnaires that have been distributed and collected. Table 2 points out the personal features of the research sample.

Table 1. The number of analyzable questionnaires distributed and collected

Number of Questionnaires distributed	Number of questionnaires collected	Number of non-analyzable questionnaires	Number of Analyzable questionnaires
220	210	10	200

Table 2. The personal characteristics of the research sample (200 individuals)

Sex				Age												Sscientific Qualification									
Male		Female		18-22		23-27		28-32		33-37		38-42		43-47		48- above		Secondary		Bachelor		Diploma		Diploma higher		Postgraduate studies	
T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%	T	%
124	62	75	38	48	24	61	31	31	16	18	9	11	6	16	8	12	6	23	12	115	58	22	11	7	4	31	16

3.2 Research Tool and Variables

The variables that are adopted in this research are represented in the preparation of the questionnaire as follows: 1. Personal variables 2- Data pertinent to dealing with computer technology, internet, using email addresses and the nature of such usage. 3-independent variable represented by: the repeated use of email accounts represented by the frequent use of email address by the user. 4-the dependent variable is represented in security and privacy of the email address. The answers of the respondents were analyzed by using Likert five-point scale as

follows: Completely agree (5), agree (4), neutral (3) do not agree (2) completely disagree (1). The arithmetic averages of the measurement tool adopted was (3), because the average answers equal of greater means agreement, while less than that value means disagree.

The results were presented to arbitrators consist of specialized professors at the University of Jordan. Their comments were taken in to accounts by paragraphs were reformulated in addition to modifications required were designed to obtains precise accurate balance between the questionnaire content and paragraphs. The internal consistency of the questionnaire validated through Cranach's Alpha coefficient in its whole final formulation and all variables. It is noted in were high as the reliability coefficient of all variables was (0.82) which a high reliability percent and acceptable for this research.

Table 3. The reliability coefficients of all variables

Variable	Reliability Coefficient
The frequent use of emails by the user	0.84
The security and privacy of email accounts	0.81

4. THEORETICAL FRAMEWORK

Dealing with the internet is often considered risky, especially the security aspect. Many users are concerned about their private information that other may have access to. Many electronic sites use e- mail as a tool of communication through the activation of subscriptions, sending invitations and information to the users. Sometimes, the email may be used as a means of promoting products of companies and sometimes the users are sorted according to their types to accomplish effective and rapid commercial targets. If this user's information is leaked, then it might be used for non-commercial purposes, which may cause his privacy be hacked.

4.1 Browsing Websites Risk

The use of the services and applications on the Internet requires the user to create an account with a user name and password. The problems pertaining to the use of the password and identified name of user as an ID are due to wrong habits followed by the user. Many researchers become more interested in these topics in the last decade; such as [6], [2], [7] and [8].

Perlman and Kaufman addressed the ongoing problems related to the use of the user name as an ID as well as the diagram of using the password and the problems generated by using the same password and user name in multi websites [7]. Aspinall in [8] discussed in his study the behaviour of the user pertaining to how to choose or design the security question as sometimes weak question and answer are used, then subsequently easily hacked.

In [9], the author pointed out that the use of the email address as an ID becomes common and replaces the use of the user name as a hobby. This leads to many benefits; First) it is easy for the user to remember his email address which is better than using multi user names as he needs to remember one email address for multi websites than using multi user names. Second) internet services providers consider it more convenient to communicate with users by using their emails collected by the steps of signing up an account. Amazon and EBay use this method. Third; the user can recover and change his password whenever he forgets his password through his email. This method is convenient and secure to the internet service providers. Many websites require the user to use his email to have access to their web pages because of the benefits mentioned herein. Despite all that, the users will face several problems relevant to the privacy and security due to

the potential of disclosure of their information to others compared to using the user name as an ID.

It is noted that some websites track the visitors' performance and save a lot of information through their visitors' files. These files contain the websites he moved from, IP, his type of account and the browser used. There is a possibility that the website might have special software that could identify the user's emails and other information. Such software can be disabled, whole or part, within the browser of the user. This would lead to limit the abilities to get the information from his personal PC by deactivating Java in the browser through the following orders: from the View menu, we choose option and then advance and then activation boxes (enable Java JIT compiler & enable Java logging) or as per the browser features, we can enable or disable java script. There are some websites working on recognition the information recorded about the user in the visited sites; such as this websites: www.consumer.net/analyze. It has a great ability to know the details of what has been stored in those visited websites. The user should be careful to divulge private information in his visits to the websites and make sure the websites is reliable and does not exchange or pass such information to another party to harm him.

It is also noticeable that many of the sites use Cookies, called (cookie) hypertext file, in the hard disk. This type of file is used to save some information about the visitor, such as the user name and password. These files are stored on the user hard disk drive, in addition to IP and the websites visited. They are often written in encrypted text files in a manner that the processors in the sites could decrypt, (https://docs.google.com). It is not necessary that cookies are used for good purposes every time, where others can see that information, which is it sacrilege to the user privacy. As we said, cookies are usually used to collect information about users, so it is preferable to clean such files after each browsing, especially non-secure sites. For example, the news sites use spaces in their websites aiming to collect comments and subscription. These spaces also require your email and save those views for a long time, where can be read by any one, so the user must be careful in his writings or information he delivers that might hurt him later [10].

4.2 Use of Passwords in the E-mail

The password in the email is very important and must be strong. It should not depend on simple words derived from a name of a city, work place, or career, so as not to be hacked easily. There are specialized programs in the market to discover the password through speculation these words several thousand times. There are also gaps in the use of electronic mail, which attackers can take advantage of them, for example, ability to remember the password automatically from programs or the possibility of saving browsing or auto completion to names or records of websites visited. With the large number of websites and services provided on the websites, we always find websites request user to enter the user name and password. The user could have been forced to do so several times a day; at work PC station, any forum he subscribed and at the end of the day, his bank account. Therefore, there must be some basics and information be developed to assist the user to remember his password by using complicated characters which cannot be hacked or detected.

Some users use one password for multi accounts, believing that using a consolidated password, which is wrong in terms of security. Suppose that someone has stolen this password, including the user's bank account, work place account, thus the thief will try to use this word in all the user accounts.

4.3 Overcome the Problem of Frequent Use of Email Account and Password

The user has to take into account not using easy peculated words, such as the first name or surname, car model or well known names as well as not to use the hones numbers or his ID number or sequence numbers or characters, such as 1234 or *abcd*. User must enter some symbols too, such as @, $,# *, to get a complicated password. For example, the word passwords can be complicated by adding symbols that cannot be encrypted, to become as p@s$w0rd. You can also use small and capital letters and insert numbers, such as A9b3C7d.

There is another way similar to the previous one, by dividing the password, according to its importance into two or three parts; main password and subsidiary. The bank account and private email passwords are classified as main passwords, while passwords used in forums or websites are classified as subsidiary. Hard strong passwords must be used for main passwords, where must include 8 characters (letters, numbers and symbols). The simple easy passwords can be used for the second subsidiary websites for their little importance. To tackle security and privacy problem, there are some programs which can save multi passwords and store that in one file, which can be encrypted and protected by one password, to facilitate saving the passwords and the user is requested to remember one password to enter into this program to review his passwords. Among these programs, "Web Confidential", "LastPass", "KeePass", in addition to free websites such as http://www.mirekw.com/winfreeware/pins.html and http://passwordsafe.sourceforget.net and http://keepass.sourceforget.net.

Some of these sites can be used in the cell phone or attach to a file in the USB flash memory.
The password must not be given to anybody, and if given or be known to anybody, you must change it promptly. The user must not write down is password and leave near his PC not on the desktop. The user must cancel auto save characteristic to save his password and change his password periodically (preferable once every 40 days). In case of suspension of virus infection, the password must be changed as precaution measurement.

User can tackle the problem of repeated use of the password by creating a special password for each account or email or websites. The user may find difficult to remember, leading to cancel his subscription in certain websites. At the same time, using one password for all accounts will make his password vulnerable, and then all his account will be lost.

Those who do not want to use this solution; they can develop a special algorithm and use it in their all accounts. Suppose that the web name is abcd.com and his name is Ahmad, he can use, for example the first three letters of his name, add number 3 and then add the last 3 letter of the web name to be ahm3cde. Whenever he wants to enter into xyz.net, he can use the algorithm as follows, but with changing the last letters to be ahm3xyz. This system is called the mask. It can be applied to all websites and accounts he subscribed, which is easy way and he needs only to remember the method and application [11]. The researchers in [12] used a graphical passwords or biological features of the user, such as fingerprint or biometric passwords [13]. The graphical one needs the user to remember the graphic of the password, while the biological type does not need the user to remember anything.

The graphical type needs, like the text one, the user to remember many graphics and has the problems the same as text one. The biological password requires special receiver devices, unlike the text one, such as the intelligent card, or the use of the cell phones to receive the password, which may not be convenient to the user, because of the probability of loss in addition to the security problems related to such devices [14]. The user may face another kind of problems concerning the password recovery. When the user creates an account, some companies, like

Yahoo, develop some additional security questions to recover the lost password, which is the answer of security question/s; such as the name of father. Some users write the real answers to such personal questions. It is preferable not to write the real answer of you father's name. for example, but counterfeited answers known only to the user in order to avoid misuse by others and trick the web by true answers to have access and the password of the user.

5. ANALYSIS AND RESULT DISCUSSION

This section looks at what we do with all the information have been collected. The analysis of focus group information can be done at a whole range of levels depending on what we want to do with the information.

5.1 Dealing with Computer, Internet Technology and Main Emails

1. Are you able to use the computer?

The results shown in table 4 indicate that all the members of a sample research have the capacity to use the computer and this is due to the method of selecting the sample by researchers, which included those who have the ability to use computers and the Internet.

Table 4. Answers to Members of the Sample on their Capacity to Use Computers

The Phrase	Yes		Not	
	T	%	T	%
Do you have the ability to use computers	200	100	0	0

2. Do you have the Knowledge to Surf Enter the Websites?

The results shown in Figure 1 indicate that (76 %) of the members of the research sample have the knowledge to surf the websites, and (22 %) have medium level, while 3% little knowledge. The results indicate that the majority of the sample members have good knowledge enables them to surf the websites well.

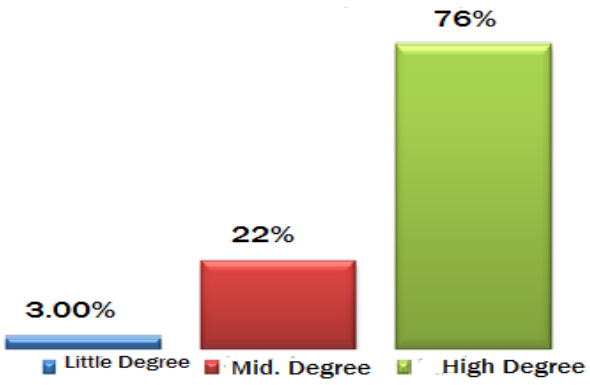

Figure 1. The answers of the research sample in respect of their ability to enter into websites

3. Do you deal with the following websites?

The results shown in the Figure 2 that the social websites came in the first order by 90%, while the digital news versions came the second by 80%, and the scientific researches websites came the third in order by 74 %, forums came forth by 59%, the e-government websites came fifth by 56%, shopping came sixth by 55% and the stock market came the seventh by 17%. Therefore, the largest portion uses the internet for social communication and news purposes.

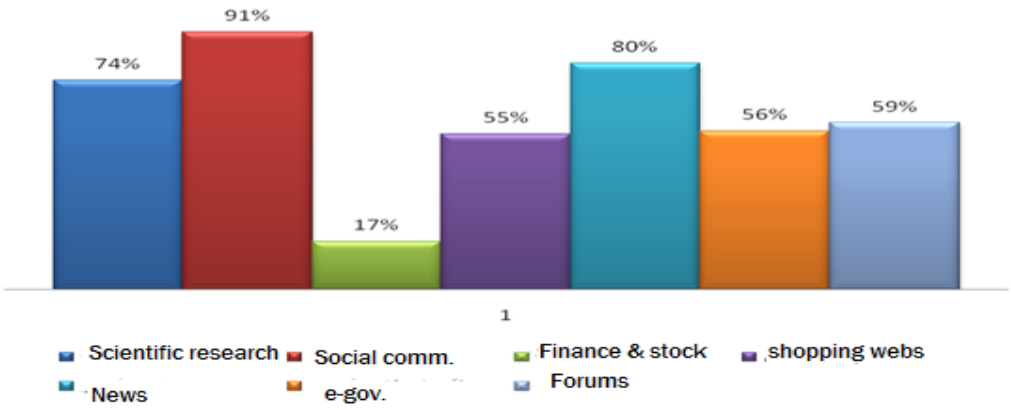

Figure 2. The proportion of users dealing with websites according to nature of websites

4. The language of the websites the users deal with:

The results shown in Figure 3 indicate that 43% of the users deal with both Arabic and foreign websites, 26 % of the users deal with Arabic websites only and 16% deal with foreign websites only. The results indicate that half of the users approximately deal with both Arab and foreign websites, which good signal to the Arab citizen and 15% of the research sample do not deal with any web, which points out that little of sample members have no certain interest to get knowledge of the websites.

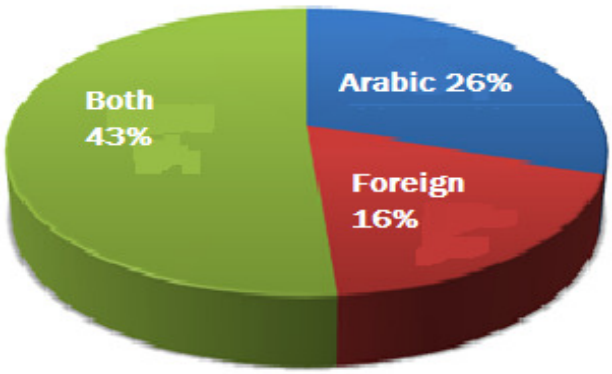

Figure 3. The language of the websites dealt by the users

5. The number of email accounts possessed by the research sample:

The results shown in Figure 4 indicate that 54% of the sample members have (1-2) email accounts, 8 % have (3-4) email accounts and 38% have more than 5 email accounts. The results indicate that more than half of the research sample have (1-2) email accounts, which reflect the reality of the Arab email users have do not have the multi accounts culture to protect their privacy; i.e. dividing them into major and secondary accounts as mentioned here in above.

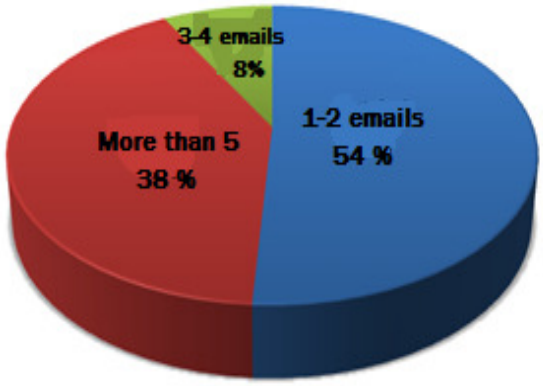

Figure 4. The Number of the Email Accounts and the Users Proportion

6. How many email accounts being used frequently:

The results shown in the Figure 5 indicate that proportion of the users who use (2) email accounts frequently was 43% which the highest, then (1) email account with 38% and the minimum proportion, 18 %, represents the users of 3 email accounts. The result is logical and reflects the general condition of the email users, which are 2 emails with frequent use.

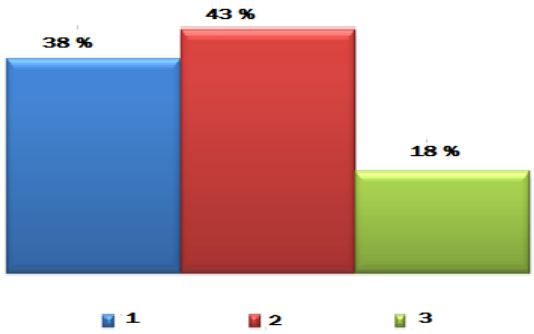

Figure 5. The Number of the Email Accounts used by the Sample Members Frequently

7. The availability of email account or work:

Figure 6 shows that 72% of the sample members have work email account at jobsite and 26% do not have. This result reflects the method of selecting the sample members which almost focused on workers at commercial and communication companies in addition to banks and university staff members who likely have email at jobsites.

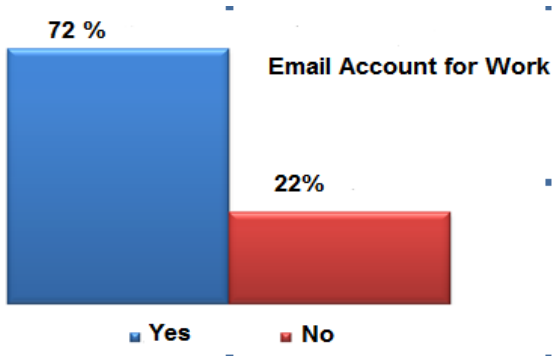

Figure 6. The Provision of Email Accounts for Work

8. The email Accounts used by the sample members:

The results shown in Figure 7 points out that 61% of the sample members use email account at Hotmail, 53% use Yahoo, 52% use the work email accounts and 31% use Gmail. These proportions reflect the real use of the email accounts of the sample members which highlight the existence of email accounts for work, which are used the highest portion of frequent use. Moreover, the majority of the sample members have personal email accounts at Hotmail and Yahoo mail.

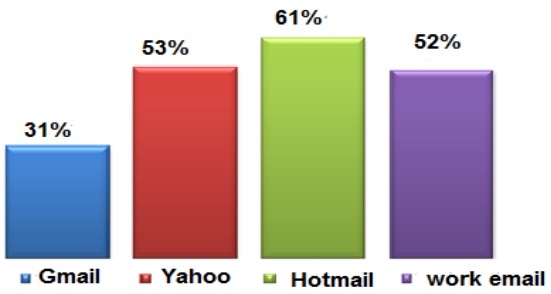

Figure 7. The email accounts frequently used by the members of the sample

9. The Method of sorting the emails by the members of the sample

The results shown in Figure 8 indicate that 47% of the members of the sample pointed out that they have "main email account to receive the emails for work only", 23% of the members pointed out that they do not have such email, while 59% of the members have a main email account for personal emails only. The proportion of those who do not have main email account was 15% while 35% **pointed** out they have secondary email for subscription in all websites only. The proportion of those who do have secondary email account was 28%. The results reveal that 30% of the sample members "do not use such division and they have only one email for all purposes". The proportion of those who use this division was 33%, i.e. they have main and secondary email accounts. The results confirm that significant proportion of users do not depend on division their email accounts, thus their privacy would be vulnerable.

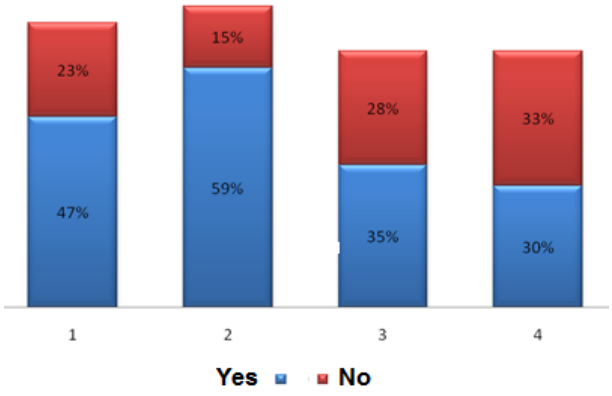

Figure 8 The answers of the members of the sample on their method of sorting their emails

5.2 Respondents answers on the phrases related to the variable of frequent use of emails

Table 5 shows the members of the sample in general do not agree on all the phrases of the variable. The arithmetic average of their answers was (2.23) with diversion standard (0.80). Their arithmetic average of their answers to the phrase No 1 of the variable, stated "When the password of a secondary email, I rely on the main email to receive the link message to password recovery", was (1.84) with diversion standards (1.87), which is less than the average of the measurement tool (3). This indicates their disagreement which positive status. The arithmetic average second phrase stated "my secondary email account always transfer all the messages to my main email" was (1.23) with deviation standard (1.41), which is less than the average of the measurement tool (3); i.e. they refuse to depend on the secondary email account to transfer all their messages to the main email, which positive status.

Table 5. The Analysis of the Research Sample Answers on the Phrases of the Variable "the Re-use/ Frequent Use of the Email"

Ser.	Phrase	Arithmetic Average	Standard Deviation
1	When the password of a secondary email, I rely on the main email to receive the link message to password recovery	1.84	1.87
2	My secondary email account always transfer all the messages to my main email	1.23	1.41
3	I always prefer to transfer the email message from the work email messages to my main email	1.77	1.55
4	I use the main email to register in all Internet sites	2.17	1.30
5	I always use the same password and user name when registering in all Internet sites	1.59	0.71
6	I use the same password and user name when registering in some Internet sites	1.92	0.57
7	I do not use the same password and user name to register in the various Internet sites	1.33	0.41

8	I use the same user name in Hotmail, Yahoo & Gmail..etc"	1.8	0.61
9	I prefer using a special email account in registering in all Internal sites (Scientific, shopping, social communication, news and e-gov. sites)	1.46	0.09
General Average of the Variable		**2.23**	**0.80**

The arithmetic average of the third phrase stating "I always prefer to transfer the email message from the work email messages to my main email" was (1.77) with deviation standard (1.55), which is less than the average of the measurement tool (3). This confirms their disagreement, which positive status. The arithmetic average of the fourth phrase, stating "I use the main email to register in all Internet sites", was (2.17) with deviation standard (1.30), which is less than the average of the measurement tool (3), which confirms their disagreement on using the main email in registering in all Internet sites, which is positive status. The arithmetic average of the fifth phrase, stating "I always use the same password and user name when registering in all Internet sites" was (1.59) with aviation standard (0.71), which less than the average of the measurement tool average. This confirms their disagreement, which is positive status. The arithmetic average of the sixth phrase, stating "I use the same password and user name when registering in some Internet sites", was (1.92) with deviation standard (0.57), which is less that the average of the measurement tool. This affirms the previous results, which is also positive status. The arithmetic average of the seventh phrase, stating "I do no use the same password and user name to register in the various Internet sites", was (1.33) with deviation standard (0.41), which less than the average of measurement tool. The result here is contrary to the previous phrases. This reveals negative status; i.e. they use the same password and user name when registering in the various Internet sites. The arithmetic average of the eighth phrase, stating "I use the same user name in Hotmail, Yahoo & Gmail..etc", was (1.80 with deviation standard (0.61), which is less than the average of the measurement tool. The results were positive.

The arithmetic average of the ninth phrase, stating "I prefer to use a special email to register in all Internet sites (scientific, shopping, social communication, new and e-gov.)", was (1.46) with deviation standard (0.09), which is less than the average of the measurement tool. This result is negative; i.e. they prefer to use special email account to register in all Internet sites. Therefore, we can summarize, according to the above-mentioned results, that the culture of protecting the emails and use them appropriately, to some extent, available among some Arabs, represented by the members of the research sample. This is obvious through the difference of the degree of their agreement about the variable phrases. In the other hand, we find contradiction in their answers, which may be due to the fact that some members were not objective in their answers, or they are not aware enough of privacy and security of their emails.

5.3 Answers of sample members on the phrases related to the privacy and security of the emails.

Table 6 shows that the member of research sample disagree on all the phrases of this variable, as the arithmetic average of their answers was (1.31) with derivation standard (0.54). The arithmetic average of the tenth phrase, stating "I cannot remember the user name and password of all my emails because of it is easy", was (1.84) with deviation standard (1.87), which is less than the average of the measurement tool (3). It is a negative status. The arithmetic average of the 11th phrase, stating "I do not think that the protection of the user name and password is relevant to the privacy and security of the user", was (1.07) with deviation standard (0.77), which is less than the average (3). This means that there no agreement among the members of the sample, which is a

positive status, indicates their awareness of the importance of protecting their user name and password. The arithmetic average of the 12th phrase, stating "I think that all Internet sites protect the privacy and security of the user to encourage him to benefit of the service provided", was (1.14) with deviation standard (0.75), which is less than (3). This affirms their disagreement, which is negative status indicates the users content that not all Internet sites protect their user's privacy and security. The arithmetic average of the 13th phrase, stating "picking simple password do not contribute in the protection of the user account", was (1.15) with deviation standard (0.88), which is less than the average of the measurement tool. This also confirms their disagreement which is positive status. The arithmetic average of the14th phrase, stating "I prefer to use multi passwords for the same email when using in subscription with the Internet sites", was (1.14) with deviation standard (0.92), which less than the average (3), indicating their disagreement. This is negative status. The arithmetic average of the 15th phrase, stating "I think that the password recovery Figure or steps adopted by all sites do not secure the privacy and security of the user", was (2.81) with deviation standard (0.17), which is less than the average (3) and it is also a negative status. The arithmetic average of the 16th phrase, stating "the request to specify question and answer of the user is known only the user adopted by Internet sites contributes to the protection of security and safety of the account", was (2.28) with deviation standard (1.40), which is less than the average of the measurement tool. It is also a negative status. This is due to the failure of the user to use a difficult question and their answers were logical as it is mentioned in the theoretical aspect.

Table 6. The analysis of the answers of the sample members on the phrases related the variable of security and privacy of the emails

Ser.	**Phrase**	**Arithmetic Average**	**Standard Deviation**
10	I cannot remember the user name and password of all my emails because of it is easy	1.055	0.65
11	I do not think that the protection of the user name and password is relevant to the privacy and security of the user	1.07	0.77
12	I think that all Internet sites protect the privacy and security of the user to encourage him to benefit of the service provided	1.14	0.75
13	picking simple password do not contribute in the protection of the user account	1.15	0.88
14	I prefer to use multi passwords for the same email when using in subscription with the Internet sites	1.14	0.92
15	I think that the password recovery Figure or steps adopted by all sites do not secure the privacy and security of the user	2.81	0.17
16	the request to specify question and answer of the user is known only the user adopted by Internet sites contributes to the protection of security and safety of the account	2.28	1.40
17	I always read the use, security and privacy policy when registering in the Internet sites	1.73	1.42
18	I do not receive many message from unknown sites just after creating account in the Internet sites which give the impression that they sell the emails of the subscribers to others	1.91	1.18
19	the use of the password consisting four numbers and letters does not secure the privacy and security of my	1.91	1.53

	email		
20	Sometimes, I give the user name and password of my account of the Internet sites to my friends to benefit from their services	2.55	0.47
21	I have the technical knowledge enough to manage the password which depends on special programming that assist to achieve the coordination between the password and user name	2.68	1.53
22	the subscription in the Internet sites makes me face the problem of hacking the emails	2.55	1.58
General Average of the Variable		**1.31**	**0.54**

Main Hypothesis Test: "There is no moral impact relation of statistical significance at the level ≤ (0.05) between the re-use of the email by the user when registering in the Internet sites and its security and privacy".

The arithmetic of the 17th phrase, stating "I always read the use, security and privacy policy when registering in the Internet sites", was (1.73) with deviation standard (1.42), which is less than the average of the measurement tool. These results were negative, indicating the lack of user awareness of the necessity to read the privacy policy. The arithmetic average of the 18th phrase, stating "I do not receive many message from unknown sites just after creating account in the Internet sites which give the impression that they sell the emails of the subscribers to others", was (1.67) with deviation standard (0.48), which is less than average of the measurement tool. This is negative status. The arithmetic average of the 19th phrase, stating "the use of the password consisting four numbers and letters does not secure the privacy and security of my email", was (1.91) with deviation standard (1.53), which less than the average of measurement tool. This result is positive. The arithmetic average of the 20th phrase, stating "Sometimes, I give the user name and password of my account of the Internet sites to my friends to benefit from their services", was (2.55) with deviation standards ().47), which is less than the average of the tool. This result is positive. The arithmetic average of the 21st phrase, stating " I have the technical knowledge enough to manage the password which depends on special programming that assist to achieve the coordination between the password and user name", was (2.68) with deviation (1.58), which is less than the average of the tool. This result is logical because the users, in general, are no specialized in IT, so it is normal they have that skill. The arithmetic average of the last phrase, stating "the subscription in the Internet sites makes me face the problem of hacking the emails", was (2.55) with deviation standard (0.73), which is less than average of the tool. This result is logical because the subscription in the Internet sites is not necessary to expose the user email to be hacked. This is affirmed by the security and privacy policy being followed. Therefore, it is obvious that users are aware of some aspect and unaware other aspects related to the protection of the privacy and security of the password and their emails. It is good indicator to the Arab user the members of the sample are a part thereof.

Tables 7 and 8 herein below show the results of the slight descending analysis test, by which the differentiation of the descending analysis results obtained to ensure the validity of the model to test the hypothesis. The data of the table 7, give evidence to the validity of the model to test the said hypothesis, because the value of moral level (0.00) is less than (0.05). It is also obvious in the same table the independent variable of repeated use of the email by the user when registering in the Internet sites has construed (0.53) the difference in the variable adopted, which is "The Protection of the Privacy and Security of the User", i.e. it is interpretable, which indicates that there is significant statistical impact to the effect of reusing the email by the user when registering in the Internet sites. The significance was good because the coefficient of definition was (50%).

This result was confirmed by the coefficient correlation between the two variables, which was (0.72).

Table 7. The results of the slight descending of the relationship between the re-use of the email by the user when registering in the Internet sites and the protection of his privacy and security

Model	Total of cells	Degree of Freedom	Average of Cells	F Value	Moral Level Sig	Variable in R2	Identification Coefficient R2	Coefficient Correlation R
Descending	57,581	1	57,581	0,00				
Remaining	50,650	198	0,256			0,532	0,532	0,729
Total	108,231	199						

The statistical results shown t-test value point out the independent variable of repeated use of email by the user when registering in the Internet sites impacts the protection of the privacy and security of the user (dependent variable), as the calculation of (t value), which is moral value at the significant level (0.05) was (0.00). So, we can conclude the following: the rejection of the Null Hypothesis at the level (0.05) stating "there is relationship of moral statistical significance affect at level ≤ (0.05) between the frequent use of the email by the user when registering in the Internet sites and the protection of his privacy and security" and the acceptance of the alternative hypothesis which indicates that there is a relation between the two variables.

Table 8. The results of the analysis of slight descending the impactful relation between the frequent use of the email by the user when registering in the Internet sites and the protection of his privacy and security

Independent Variable*	B Value	Deviation Error	Beta	t- Calculated value	Significant moral level
Re-use of the email by the user when registering in the Internet sites	2,809	0.73		38,378	0.00
	-0.606	0.40	0.729	- 15.003	0.00

*The dependent variable: the Protection of the User Privacy and

6. CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions

The results of data analysis related to the variables of the research and the tests of the hypotheses, the following results can be concluded:

1-In respect of the variable concerning the dealing with computer technology, Internet and use of email accounts; the result indicate the following:

- All the research sample members are able to use the computer
- The social communication websites are the first in the order of using, while finance and stock sites became the last.
- The highest proportion deals with Arab sites and very low percent of the sample members do not deal with any site. This indicates that little are not interested to get knowledge online sites.
- The results reveal that more than half of the sample members have 1-2 email account This result reflect the facts of the Arab users of emails; i.e. they do not have the culture of multi accounts to protect their privacy by dividing such sites into main and secondary as discussed in the theoretical framework.
- The results show that the proportion of frequent email users (2) was the highest and lowest is those who use (3) email accounts. The result is logical reflects the status of the email users.
- The results highlighted that the majority of the research sample members have work email. This is refection to the way the sample was selected, which focused on those who have work emails.
- The results pointed out that the highest portion of the email users uses Hotmail and the lowest uses Gmail.
- The results pointed out that the highest proportion of users who have work emails to receive their personal emails and high proportion of users have main email to receive personal message. High per cent of the members have subsidiary email account for subscription in Internet sites only. The results also reveal that high proportion the sample members do not used such division of emails and get only one email. This results affirm that not high percent divide their emails into which make their email vulnerable.

2- In respect of the frequent email use variable: it was found that the sample members, in general, disagree with all the phrases of this variable with arithmetic average (2.23) and deviation standard (0.80). Their answers were are positive and negative on the phrases of the variable according to the results statistical analysis shown in the research context.

We can conclude that the main email protection and appropriate use are, to some extent, are available to the Arab users, represented by the sample members better than the past in most aspects, which is revealed through the differentiation of their agreement on the phrases of the variable.

3-In respect of the Privacy and Security of the emails Variable: it was found that the sample members, in general, disagree with all the phrases of this variable with arithmetic average (1.31) and deviation standard (0.54). Their answers were are positive and negative on the variable phrases according to the results statistical analysis shown in the research context. These results confirm the results of the frequent use of email variable analysis.

4-The results of analysis the main hypothesis "there is no moral impactful of statistical significance relation at the level $\leq$ (0.05) between the frequent use of the email by users when registering in the Internet sites and the protection of his privacy and security" indicate that there is a impactful relation of statistical significance between the frequent use of the email by the users when registering in the Internet sites and the protection of his privacy and security. The result was so great because the definition coefficient was (0.53) which is more than 50 percent to confirm the good coefficient correlation between the two variables which was (0.72).

6.2 Recommendations

6.2.1 Recommendations relevant to the result of the field research

The users who use their emails frequently should not use the same password and user name when registering in the Internet sites to protect their privacy and security and to use only one (private) email to register in the Internet sites (scientific, shopping, social communication, news and e-gov.).

The user must not pick easy words to their user name and passwords for all their online accounts for easy hacking, which endanger protect their privacy and security. Be sure that the sites are able to maintain privacy and security of the users through reading the privacy and security policy by which the user is encourage to benefit their services, the use of multi passwords for the same account when subscribing with Internet sites, make sure that the password and user name recovery system of the site guarantee the privacy and security of the user, reliance on the question and answer related to user only known to the user when registering in the internet sites, and be sure that such site don't give the user account to others.

Do not use the service of transferring the messages from multi accounts to the main email account for the protection of user and keep him away from the risks of transfer process because the risks of the secondary accounts may exposed might transfer to the main account during transfer process.

6.2.2 The Recommendation Related to the Subject of the Research

In the behaviour of re-using the same email with the same password and user name in multi internet sites, user has to understand that there are two aspects control the determination the password; its length and then complexity. There are certain rules, agreed by many researchers, should be followed in writing any password [6] and [2], namely:

- The password must not be sorter than 8 characteristics and not to exceed 14.
- The password must contain four elements; symbols, capitals, small letters, and numbers.
- If you use a capital letter, it must be placed at the beginning or end of the password.
- Do not use your name or a part of your email in the password.
- There are many secure sites which may save the passwords.
- Do not use a password easy detected from your life in the communication sites; such as band name, date of birth or phone number.
- User when surfing web pages must be sure that the web use SSL (Secure Socket Layer) Technology, which is used to encrypt the data and assist to save the password in the web, and keep away from websites do not use such technology.
- Never store your personal confidential data in the same website, according to [15], in order to protect your privacy and security of the email, to be used whenever he wants to enter a web, but to use the Federate Identity System by adding a third party to store his confidential data and these information are encrypted when stored [15]. Encrypt system is call knowledge protocols zero aims to secure the information from detection. The danger still exist in case that system is hacked, then all private information of the user in all sites will be vulnerable. Therefore, this system must be well designed to achieve high confidentiality [16].
- 9- Schechter in [17] proposed a solution to manage the user ID as he used a system he called (Social-authentication for identifying users). The system depends on questioning trusty people selected by the user to verify the information of a third party account when the user wishes to enter into the system, but he problem how can we find those people

(third party) on time. This problem can be overcome by the intelligent phones connected to internet or any device connected to Internet.

REFERENCES

[1] Felten, Edward W& Gaw, Shirley, (2006)" Password Management Strategies for Online Accounts" Proceeding SOUPS '06 Proceedings of the second symposium on Usable privacy and security Pages 44 - 55 ACM New York, NY, USA.
[2]Florence, Dinei & Herley, Cormac, (2007) "A large-scale study of web password habits" Paper presented at the 16th international conference on World Wide Web, pp.657–666, 8–12 May, Banff, Alberta, Canada.

[3] Shay, Richard J. K& Spantzel Abhilasha Bhargav & Bertino, Elisa, (2007) "Password Policy Simulation and Analysis" Proceeding DIM Proceedings of the 2007 ACM workshop on Digital identity management ACM New York, NY, USA.
[4]A Study of the Internet Users and Privacy of Internet sites (the Saudi Ministry of communication and IT) conducted by Information Security Team.

[5] Takabi, Lei Jin, Hassan and Joshi, James B.D, (2011)" Analyzing security and privacy issues of using e-mail address as identity" International Journal of Information Privacy, Security and Integrity, Vol. 1, No. 1.

[6] Florêncio, D., Herley, C. and Coskun, B. (2007) "Do strong web passwords accomplish anything?",in Proceedings of the 2nd USENIX Workshop on Hot Topics in Security, pp.1–6, 7 August, Boston, MA, USA

[7] Perlman, R. and Kaufman, C. (2008) "User-centric PKI" in Proceedings of the 7th Symposium on Identity and Trust on the Internet, 4–6 March, pp.59–71, Gaithersburg, MD, USA.

[8] Aspinall, D.& M Just, (2009) "Personal choice and challenge questions: a security and usability assessment" in Proceedings of the 5th Symposium on Usable Privacy and Security, pp.1–11, 15–17 July, Mountain View, CA, USA.

[9] Jin, L. (2010)" Investigations of Users' and Websites' Behaviors" available at www.sis.pitt.edu/~leijin/investigation.htm (accessed on 1/9/2010)

[10] Sophos "Security at risk as one third of surfers admit they use the same password for all websites", [Online Document][cited 2010 July 14] Available HTTP.

[11] http://www.abunawaf.com/post-5283.html

[12] Everitt, K.M. & Bragin, T., Fogarty J. & Kohno, T. (2009) "A comprehensive study of frequency, interference, and training of multiple graphical passwords", in Proceedings of the 27thinternational conference on Human factors in computing systems, pp.889–898, 4–9 April, Boston, MA, USA

[13] James, L.W. (2008) "Biometrics in identity management systems", IEEE Security and Privacy, Vol. 6, No.2, pp.30–37.

[14] Liao, K.C., Lee, W.H., Sung, M.H. and Lin, T.C. (2009) "A one-time password scheme with QR-code based on mobile phone", in Proceedings of the 5th International Joint Conference on INC, IMS and IDC, pp.2069–2071, 25–27 August, Seoul, Korea.

[15] Bertino, E., Paci, F., Ferrini, R. and Shang, N. (2009) "Privacy-preserving digital identity management for cloud computing", IEEE Data Eng, Vol. 32, No.1, pp.21–27.

[16] Camenisch, J. and Herreweghen, E.V. (2002) "Design and implementation of the idemix anonymous credential system", in Proceedings of the 9th ACM conference on Computer and Communications Security, pp.21–30, 18–22 November, Washington, DC, USA.

[17] Schechter, S., Egelman, S. and Reeder, R.W. (2009) "It's not what you know, but who you know: a social approach to last-resort authentication", in Proceedings of the 27th International Conference on Human Factors in Computing Systems, pp.1983–1992, 04–09 April, Boston, MA, USA.