

Effect of security and Trust on Email Usage

Case Study at University of Bahrain

Resala A. AlAdraj
Department of Computer Science
University of Bahrain
Manama, Bahrain
raladraj@uob.edu.bh

Mike Joy
Department of Computer Science
University of Warwick
Coventry, UK
m.s.joy@warwick.ac.uk

Abstract — In this paper, the researchers present a novel framework which derives from the TAM model by testing security and trust effects on the ease of use and on usefulness. A “one shot” case study has been conducted using a new secure email instructional model in order to validate the framework. The study found that security and trust affects the perceived usefulness, and that in turn this leads to ease of use regardless of which type of email client is used. Evidence suggests that the model may be a suitable solution for increasing the usefulness of email in computer supported collaborative learning, and can help to strengthen communication between faculty and students.

I. INTRODUCTION

Technology can offer the means for students to communicate via email and use the Internet for research, and can also help teachers familiarize themselves with students’ varying learning styles. Skilled students can explore subjects in more complexity than the basic syllabus and they can work with their own limits. Zhang and Hong [10] note the use of technology in supporting students’ access to information and further observe the motivating effect of email in helping students to improve their reading and writing skills and to communicate over distances.

Hubona & Burton-Jones [9] note that a benefit of the Technology Acceptance Model (TAM) is its ability to predict “whether users will ultimately use software applications based upon causal relationships among belief and attitudinal constructs that influence usage behaviour”, and further note the variety of email applications available. Hubona & Burton-Jones [9] have applied TAM to assess the user acceptance and voluntary usage of a particular email application, cc:mail, in two different organizations, and comment “The results largely validated TAM, although the findings suggested that certain external variables – namely length of time since first use, and level of education – directly affect email usage behaviour apart from their influence as mediated through the perceived usefulness (PU) and perceived ease of use (PEOU) constructs.”

Using their framework as shown in Fig. 1, the authors have identified the following 6 hypotheses to test.

- H1: Secure email is related to perceived trust of email.
- H2: Secure email is related to perceived ease of use of email.
- H3: Trusted email is related to perceived ease of use of email.
- H4: Perceived ease of email use is related to perceived usefulness of email.
- H5: Perceived ease of email use is related to actual usage of email.
- H6: Perceived usefulness of email is related to actual usage of email.

The authors have conducted a “one shot” case study in order to test the hypotheses and validate the framework.

The case study is an appropriate research methodology, and Yin [13] notes its effectiveness “... when the boundaries between phenomenon and context are not clearly evident”, and observes that the case study is a comprehensive approach which covers many aspects logic of design, data collection techniques, and specific approaches to data analysis.

Section II describes existing work on email usage in learning, paying particular attention to security solutions using email. This is followed in section III by details of an experiment that was conducted with students at the University of Bahrain (UOB), the results are discussed in section IV, and section V concludes.

II. LITERATURE REVIEW

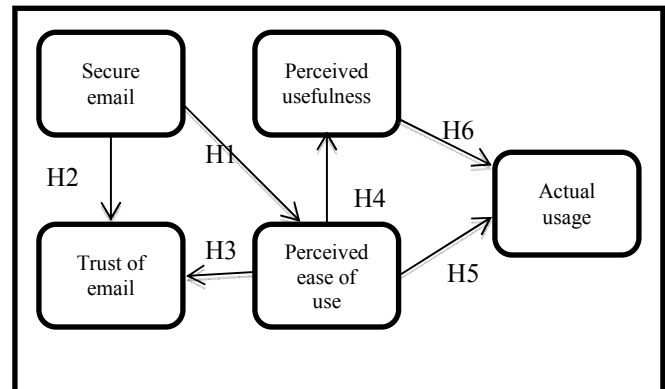


Fig. 1: The research framework (email acceptance model) (Hubona & Burton-Jones, 2003)

This section provides an overview of related published papers and covers the technical aspects of the security technologies, including trust, spam and phishing. A critical review of the literature identifies the questions that are the basis for this research.

A. Email Security concepts

Despite the age of email, concepts have changed little, the main protocols for message format and routing remain the same [4].

The first emails did not have any security services and the policies were limited. With evolving threats, new security objectives and security properties have been identified. The following are the security properties of the security services which have been identified by Cailleux et al. [4], and which require the use of cryptographic signing and encryption services:

- Non-repudiation of origin;
- Data integrity;
- Data origin authentication;
- Data confidentiality;
- Authorization.

Pretty Good Privacy (PGP), which uses a public key infrastructure and a decentralised “web of trust” model) and Secure/Multipurpose Internet Mail Extension (S/MIME) based on a centralised trust model) are common protocols which provide email signature and email encryption.

B. Trusted emails

Almadhoun et al. [3] conducted a study in order to identify the effect of security, privacy, and trust in Social Network Sites (SNSs) for the purpose of sharing information and developing new relationships in order to discover how they affect students’ enrolment. In doing this, they conducted a survey of 66 participants, and their findings suggested that perceived privacy and perceived trust in other members in SNSs is significantly related with information sharing. Furthermore, members’ trust in SNSs and its members positively associated with development of new relationships, which is positively associated with students’ enrollment and employees’ application in HEIs. However, no significant impact from information sharing to develop new relationships in SNSs was detected.

C. Spam and Phishing

Spam has great impact on emails, by challenging the safety and usefulness of email, in addition to costing time and money, and has been defined by Solic et al. [12] as “unwanted and unsolicited email, that has usually been sent to many recipients.” Spam is considered the major source for flooding

network traffic as noted by Ghafoor et al. [7] who also observed that spam creators abuse authorization weaknesses of the original email standard in which anybody can send email to any other user.

Spam can contain attachments that contain text, images or URLs and these are responsible for phishing attacks. Also, spam can contain executable files, such as viruses, worms or Trojans. Email usage has been increasing along with the growth of such unwanted side effects, and spam and fraudulent email messages are now major concerns for email users. Dhanaraj & Karthikeyani [5] clearly state “Spam was once just an annoyance, but it has now become the tactic of choice for online deception, fraud, and abuse. The freedom of communication is being misused and has become a threat to email communication society”. They report a 10% increase in spam emails in 2009 and that spam accounted for 92% of all emails sent in that year, and further note that these statistics were likely to increase rapidly.

Recently, numerous filters have been developed to detect or prevent text-based spam mails. However, some spammers put their spam contents into images in order to bypass text based anti-spam filters. There are many categories of spam, including product advertisement, financial, adult, internet, health, etc. but the email attacks that appear to be from a well-known organization are referred to as “phishing”. Phishing is one of the methods that fool people into revealing their personal information, such as personal identity data and financial account credentials, by using social engineering and technical tools without using any of the common fraud methods such as sniffing, Trojan horses or viruses. Phishing is one of the most effective online scams and is a crime in most countries, since it costs businesses millions of dollars yearly in addition to loss of personal client data. Salem et al. [11] have listed different kinds of phishing techniques including impersonation, forward attacks, pop-up attacks, voice phishing, and mobile phishing.

III. EXPERIMENT DETAILS

For the purpose of the research, the first, and perhaps most important step, was to set up email security practices for the student participants. The researchers developed a training prototype, and the experiment took three weeks for three different classes of students of different levels. The experiment was divide into three stages, and the following are the experiment stages in detail.

A. Ptototype stages:

Stage 1: Grouping the students

- The participants in each class were distributed into groups according to the project group that had been assigned by their teacher at the beginning of the term.
- The participants were asked about their frequent webmail usage.

Stage 2: Training program

- Security settings, which will be discussed in the next section, were distributed among the students.
- The participants were allowed to follow the guidelines for the security settings for a single time with the help of the researcher.
- The participants were allowed to communicate with each other by emails in the class and at home.
- Their teacher changed her office hours from face to face to email communication.
- The teachers distributed their assignments by email.

Stage 3: Follow up

In order to allow the researcher to follow up the participants, the following procedure was implemented.

- The researchers and the course teacher received copies of participants' emails as "CC".
- Follow up sheets were distributed among the participants as shown in Figure 2 in order to follow up the participants during the experiment. The sheet asked the students to fill in the following details:
 - Time of receiving/sending email;
 - Purpose of the emails;
 - Webmail type;
 - Type of email attacks;
 - Type of action taken.
- Additionally, the researcher followed them up by using a phone chat application (Whatspp).

[illegible]

Fig. 2: Follow-up sheet

B. Prototype design

The training program of the prototype included both pedagogical and technical guidelines, and the “How to secure Gmail and Hotmail” guidelines were distributed amongst the participants. The researchers chose the following most important, common and straightforward security processes.

1- Two-step verification

This step helps protect an email account by making it more difficult for a hacker to sign in by prompting the user to enter a security code to sign in. Then a new security code is sent to the user's phone or alternative email address. This step uses two methods of verifying the user's identity when they sign in to their email account: password and an extra security code.

2- Enabling HTTPS security

HTTPS encrypts the data sent and received with SSL, while HTTP sends it all as plain text. The participants were asked to always use “https://” in the URL address in order to secure their data. This process is explained in the guidelines.

3- Checking account activity

The command “Last account activity” can check for suspicious logins and password changes. For example, in Gmail this command appears below the inbox. Participants were particularly instructed how to check “Junk emails” for deleting junk mails and stopping spam. Participants were also educated on reviewing tagged or filtered messages to identify ones that have been incorrectly labeled.

4- Filtering

The researchers trained the users to configure filtering features such as creating lists of safe senders and lists of senders to block.

5- Creating labels

This step is to create folders in which to organize incoming and outgoing emails and course materials.

6- Demonstrating email tasks

This step allowed the user to perform the tasks related to an email message the user received.

7- Starring items

Users can star the emails messages to easily mark certain messages as important or to indicate which ones need to be replied to later.

IV. METHODOLOGY

Throughout this study, the researchers were aware of the need to gather only sufficient, legal and reliable data that were relevant to the work, and not to be hampered with unnecessary data. Both quantitative (questionnaire survey) and qualitative methods were used to collect the data.

A. Questionnaire survey

The researchers developed a questionnaire to be distributed amongst the participants at the end of the case study to collect the participants' perceptions. There were 32 questions altogether in the questionnaire, grouped into seven sections according to the questions aspects. The details of each question are described below.

The first section of the questionnaire aimed to discover the demographic background of the students, with questions covering age, year of study, course, etc. The second section obtained information regarding the types of webmail the students used during the experiment.

The eight sub-questions in the third section focused on measuring each participant's perception of how secure their frequent emails were during the experiment. The sub-questions used a five-point Likert scale and were derived from the email security settings, which were given to the students during the experiment so that they could apply them to their emails.

The questions in the fourth section measured the frequency of email usage by the students during the experiment using (never, rarely, occasionally, often) measurements.

The questions in the fifth section measured how much the participants trusted the emails they received after setting the security during the experiment. The questions were derived from McKnight et al. [6].

Section six measured perceived usefulness of email during the experiment using a five-point Likert scale of (strongly agree, agree, undecided, disagree, and strongly disagree). This section included six questions which were adapted from Hubona and Burton-Jones [9]. Finally, section seven similarly measured perceived ease of use during the experiment.

B. Construct validity

The researchers have scrutinized the construct validity of the instrument to ensure that each item measures what it is intended to measure [1]. The aspects of the questionnaire such as trust, perceived ease of use, perceived usefulness and actual usage were taken from journals and articles cited in Section II. Security guidelines were derived from the "security settings" of Gmail and Hotmail. Furthermore, the researchers made a comprehensive review of previous attempts to measure the variables that were investigated in the present study.

C. Face validity

The questionnaires were presented to a panel of judges consisting of 10 faculty members from the IS Department in the IT College at UOB, and a statistician who works as a vice director at the scientific publishing center.

D. Pilot testing

Pilot testing was conducted to test the validity and the reliability of the questions used in the questionnaire. Cronbach Alpha was used for the assurance of reliability of the four dimensions of the instrument. Twenty-five students studying at UOB selected at random were asked to respond to the

questionnaire items. Table 1 shows reasonable internal consistency for three dimensions of the instrument; these were: trust (0.806), usefulness (0.801), and ease of use (0.775). The security dimension reliability was 0.649, which is acceptable.

This was deemed to be acceptable, and was not changed because, in order to identify the participants' perceptions of the practice tasks, the security items in the questionnaire must be based on the security settings that are available within the webmail services.

TABLE 1: INTERNAL CONSISTENCY

No. of sections	Factor	Cronbach's Alpha	No. of Items
3	Security	0.649	8
5	Trust	0.806	8
6	Usefulness	0.801	6
7	Ease of use	0.775	6

E. The Sample

After validation, with some minor adaptations and amendments, the questionnaires were distributed to 100 students in the available classes. The pilot respondents were discarded in the main study. The researchers received 91 responses only. The sample was chosen randomly from students in the IS Department in the IT College at UOB.

V. DATA ANALYSIS

Quantitative data provided us with quantifiable results, and data collected through tools such as the questionnaire were analyzed using SPSS software. Descriptive as well as analytical statistics were used. Correlation coefficients, means and standard deviations were obtained.

A. Descriptive analysis

The researchers analyzed the email clients used during the experiment, and as illustrated in Table 2 that the most frequently used email by the participants was Hotmail (40.7%). The second was Gmail (34.1%). However, Yahoo is the least used.

TABLE 2: FREQUENCY DISTRIBUTION OF WEBMAILS USED DURING THE CASE STUDY

	Frequency	Percent	Valid Percent	Cumulative Percent
Often	8	8.8	8.8	8.8
Occasionally	42	46.2	46.2	54.9
Rarely	28	30.8	30.8	85.7
Never	13	14.3	14.3	100.0
Total	91	100.0	100.0	

Table 3 shows that 46.2% of the participants indicated that they have used email for learning occasionally, and about one third (30.8%) rarely. However, 8.8% of the participants used email for learning regularly.

TABLE 3: ACTUAL EMAIL USAGE DURING THE CASE STUDY

Webmail's type	Frequency	Percent	Valid Percent	Cumulative Percent
Yahoo	9	9.9	9.9	9.9
Gmail	31	34.1	34.1	44.0
Hotmail	37	40.7	40.7	84.6
Gmail + Hotmail	14	15.4	15.4	100.0
Total	91	100.0	100.0	

B. Hypotheses testing

In order to answer the above research questions and to test hypotheses 1 to 5, the researchers used a questionnaire to gauge the student perceptions in relation to secure email usage. Pearson correlation was used to test the hypotheses in section 5 to find out whether hypotheses 1 to 5 are accepted. The Pearson coefficient was chosen as it is the most common and usable proposition for normal distributed data [1].

Table 4 shows that the correlation between secure email and perceived ease of use and trust of emails were found to be 0.502 and 0.575 respectively; which are highly significant ($\alpha=0.01$). Thus, the first and second hypotheses (1 and 2) of the study are accepted, and we conclude that secure email and both 'perceived ease of use' and 'trust' are positively correlated.

Furthermore, the correlation between trusted emails and perceived ease of use was found to be 0.614 which was found to be significant ($\alpha=0.01$). Thus the third hypothesis (3) of the study is accepted and we conclude that trusted email is positively related to perceived ease of use of the email.

In relation to hypothesis 4, which stated that perceived ease of use is related to perceived usefulness of email, as shown in the Table 3, it is evident that the correlation between them (0.452) is significant ($\alpha=0.01$). Thus, hypothesis 4 is accepted.

Table 4 shows that the correlation between ease of use and actual use was found to be -0.215 which was found to be significant ($\alpha=0.05$). It is evident that hypothesis 5 is accepted but with negative correlation. This means that perceived ease of use is negatively related to actual usage of email.

TABLE 4: PEARSON CORRELATION COEFFICIENTS BETWEEN THE TARGETED VARIABLES

Secure email	trust	Perceived usefulness	Perceived ease of use	Actual usage	Secure email
Secure email	Pearson Correlation	1	.575**	.420**	.502**
	Sig. (2-tailed)		.000	.000	.000
	N	91	91	91	91
Trust	Pearson Correlation	1	.519**	.614**	-.183
	Sig. (2-tailed)		.000	.000	.083
	N	91	91	91	91
Perceived usefulness	Pearson Correlation		1	.452**	-.189
	Sig. (2-tailed)			.000	.073
	N		91	91	91
Perceived ease of use	Pearson Correlation			1	-.215*
	Sig. (2-tailed)			.000	.040
	N			91	91
Actual usage	Pearson Correlation				1
	Sig. (2-tailed)				
	N				91

However, from Table 4 the correlation between perceived usefulness and actual usage was found to be -0.189, which was found not to be significant ($\alpha=0.01$ and $\alpha=0.05$). We can conclude that hypothesis 6 is rejected. Thus, perceived usefulness is not related to actual usage of email.

VI. CONCLUSION AND DISCUSSIONS

The researcher conducted a one-shot case study as identified earlier in the paper to validate the contextual framework and to answer to test the hypotheses listed above. The following conclusions were driven from the hypotheses testing.

H1 and H2: Perceived ease of use and trust of the email are both positively correlated with secure email.

H3: Trusted email is positively related to perceived ease of use of the email.

H4: Perceived ease of use is positively related to perceived usefulness of the email.

H5: Perceived ease of use is negatively related to actual usage of email.

H6: Perceived usefulness is not related to actual usage of email.

Thus, the framework depicted in Fig. 1 has been validated for only hypotheses 1 to 4. In other words, the researcher can confirm that secure email and trusted emails lead to ease of use, which in turn lead to usefulness. Moreover, ease of use relates to usefulness which is already validated. However, the result of this case study clashes with Hubona & Burton-Jones [9] because H5 was accepted but with negative correlation. In other words ease of use and usefulness have a significant relationship but it is negative which cannot validate the framework. Additionally, H6 is rejected, thus there is no relationship between perceived usefulness and actual usage of email. Therefore, we can conclude that the research framework is not validated. Moreover, descriptive analysis shows that many of the participants indicated that they have used email for learning occasionally, and about one third (30.8%) rarely. However, 8.8% of the participants used email for learning regularly. Additionally, the email service used most frequently by the participants was Hotmail (40.7%).

The case study found that security provided by webmails and students' trust affects the perceived usefulness of webmail, and that in turn leads to ease of use regardless of which type of email client is used. However, it was not proof that usefulness affects the usage of email. Evidence suggests that the model may be a suitable solution for increasing the usefulness of email in Computer Supported Collaborative Learning (CSCL), and can help to strengthen communication between faculty and students.

REFERENCES

- [1] K. Alkhalili. Validity of research framework. [Interview]. 15th April 2014.
- [2] K. Alkhalili Validity of the instrument. [Interview]. 4th March 2012.
- [3] N.M. Almadhoun, P.D.D. Dominic, and L.F. Woon. "Perceived security, privacy, and trust concerns within Social Networking Sites: The role of Information sharing and relationships development in the Malaysian Higher Education Institutions' marketing," *Control System, Computing and Engineering (ICCSCE)*, 2011, pp. 426-431.
- [4] L. Cailleux, A. Bouabdallah, and J.M. Bonnin. "A confident email system based on a new correspondence model," *Proc. 16th Int. Conf. on Advanced Communication Technology (ICACT)*, Feb. 2014, pp. 489-492. <http://dx.doi.org/10.1109/ICACT.2014.6779010>
- [5] S. Dhanaraj, and V. Karthikeyani. "A study on e-mail image spam filtering techniques," *Proc. 2013 Int. Conf. on Pattern Recognition, Informatics and Mobile Engineering (PRIME)*, Feb. 2013, pp. 49-55. <http://dx.doi.org/10.1109/ICPRIME.2013.6496446>
- [6] D.H. McKnight, V. Choudhury, and C. Kacmar. "Developing and Validating Trust Measures for e-Commerce.Information system Research," *Information Systems Research*, 13(3), 2002, pp.334-359.
- [7] A. Ghafoor, S. Muftic, and G. Schmölzer, "Design and implementation of the Secure Email System," *Proc. 1st Int. Workshop on Security and Communication Networks (IWSCN)*, May 2009, pp 1-6.
- [8] Y.-Z. He, C. Cheng, Q.-S. Xu, and L.-H. Yang. "A research on methods and applications of case study in public administration," *Int. Conf. on Management Science & Engineering (ICMSE)*, Wuhan, Aug. 2014, pp. 1977-1982. <http://dx.doi.org/10.1109/ICMSE.2014.6930478>
- [9] G.S. Hubona and A. Burton-Jones. "Modeling the user acceptance of e-mail," *Proc. 36th Annual Hawaii Int. Conf. on System Sciences*, Jan. 2003. <http://dx.doi.org/10.1109/HICSS.2003.1173675>
- [10] N. Zhang, and B. Hong. "Research on Computer Technology for E-learning in Higher Education." *Proc. Int. Conf. on e-Education, e-Business, e-Management, and e-Learning, (IC4E '10)*, Jan. 2010, pp. 295-298. <http://dx.doi.org/10.1109/IC4E.2010.125>
- [11] O. Salem, A. Hossain, and M. Kamala. "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks," *Proc. 10th IEEE Int. Conf. on Computer and Information Technology (CIT)*, Jun. 2010, pp. 1418-1423. <http://dx.doi.org/10.1109/CIT.2010.254>
- [12] K. Solic, D. Sebo, F. Jovic, and V. Ilakovac. "Possible decrease of spam in the email communication," *Proc. 34th Int. Convention (MIPRO)*, May 2011, pp. 1512-1515.
- [13] R.K. Yin. *Case Study Research: Design and Methods*. Newbury Park, CA: Sage. 1984.