Users' Awareness of Visible Security Design Flaws

Maha M. Althobaiti and Pam Mayhew

***Abstract*—Financial websites incorporate critical security features, as they require a high level of security. Users sometimes need to respond to security indicators in order to make security decisions. These decisions are usually based on users' understanding of security features that may affect safety and privacy. This paper examines users' awareness of security features in banking websites. These features include security indicators (warnings), insecurely e-mailing security information, providing biometric information, and responding to warning messages. A total of 100 users were enrolled in the experiment. Users were asked to initiate a banking transaction following a realistic scenario in a simulated online banking platform. During the experiment, users had to respond to security indicators, and their reactions were observed and analysed in depth. The results demonstrated that none of the participants looked at the address bar to find a lock icon or the website address indicator 'https', the absence of which indicates a potentially insecure connection. The results from examining users' responses to warning messages revealed that most users responded to individual messages without concern or careful reading to understand a message's content. Moreover, the study was the first to the authors' knowledge that examined users' awareness of the risks of providing biometric information (such as the fingerprint). The results indicate that three out of 100 users were concerned about providing their fingerprints and refused to allow their fingerprints to be saved in any kind of database.**

***Index Terms*—E-banking, security, usability, warning message.**

I. Introduction

E-banking has become a mass-market product, with an increasing number of online customers who rely upon the ease of use of online banking platforms for a wide variety of transactions. The need exists to protect the data online banking customers provide (and their overall banking data) again unauthorised users, as much of these data are sensitive and the number of attacks is expected to increase. Authentication or user identification is an effective approach to enable successful authorisation for the user. Several authentication mechanisms exist to provide the user with successful verification. The main challenge in many cases is users' awareness and understanding of how to use these methods effectively and correctly in a sensitive environment. Of particular interest is how users will interact with security features within the sensitive online banking environment. The authentication process needs to be investigated further, as evidence regarding users' understanding (or lack thereof) of security features is scarce.

Security features refer to features that may be present during the online banking authentication process. They include warning messages that help users mitigate possible risks, requests to provide biometrics information and visible or notable security design flaws (including availability of SSL warnings and the need to send information from an insecure page).

The general proposition for this study is that users are generally unaware of security indicators or of how to make responsible decisions in an online environment with these indicators. To confirm this, the current study investigates users' understanding and awareness of security features.

This report is structured in the following manner. Section II introduces the security warning indicators and presents relevant works in the field of information security awareness. In Section III, we will describe the methodology used to conduct the experimental study. The last section concludes with the results and discussion.

II. Literature Review

A. Security Warning

Wogalter in [13] defined 'warning' as a safety communication used to warn users about threats and risks to be minimised or avoided. Tuchscheerer in [11] provides a different definition: a warning is a way to draw users' attention to an action that may result in harm to the user. Users being aware of where their attention is being directed with respect to security warnings is considered one of the factors that can be measured during the execution of a security task [4]. Wogalter in [13] characterises the four functions of a security warning by stating that security warnings work as a mechanism that provides users with safety information, encourages users to behave safely, reduces potential problems and helps remind users about expected danger. These functions highlight the effectiveness of warning indicators and the extent to which they may help users avoid potential risk. The concept of security awareness in computing researches connected with the adherence of security policies for example the authors in [10] described awareness in using security program as an affective way that used to reduce system risk.

Several studies have been conducted in the field of security features and indicators. In [2] the authors conducted an empirical study to investigate the effectiveness of phishing warnings by simulating a spear phishing attack with 60 participants. The results of this study revealed that 97% of the participants failed to understand at least one of the phishing messages. Another in [8] investigated the effectiveness of security warnings via a case study of Microsoft Internet Explorer. In their study, 114 users with access to Microsoft Internet Explorer were requested to install an insecure

Manuscript received March 10, 2016; revised May 26, 2016.

Maha M. Althobaiti and Pam Mayhew are with the University of East Anglia, UK (e-mail: M.Althobaiti@uea.ac.uk).

ActiveX component. The focus of the study was whether such security warnings would prevent users from insecure actions (rather than mere observation of users' behaviour and understanding). The results showed that the warning indicator was successful to warn the users from insecure installation but it did not prevent it. Another study by Sharek and others in [9] attempted to determine which visual design of warning messages best alerted users about a potential risk. They provided the users with three fake popup windows that contained a text warning following the standard error messages provided in Windows XP, but each fake popup had a different design. They observed participants' responses to each fake message and compared these to responses to the real message. On the basis of individual users' reactions to these popup warnings (such as 'close', 'minimize', or 'OK'), the study results indicated that users did not understand the potential risks involved. 73% of the participants responded to the fake popup incorrectly. In [14] the researchers conducted a study with 30 users to evaluate the effectiveness of three security toolbars and other security indicators including status bar and browser address; they found that all three toolbars failed to protect users from potential risks and harms. Although the authors aimed to design a realistic scenario that didn't make security a primary goal for the subjects, they introduced the study to the users by stating that the goal of the study was to test security indicators, which may have affected the results.

The researchers in [12] conducted a study with 16 participants to examine users' attention to browser security, using an eye tracker to gather data. They found that users did not pay attention to web security indicators and suggested several improvements for the design of the certificate data so that these indicators could be meaningful to users. In [5] the authors conducted a study using an eye tracker to examine users' attention to security indicators. Their study was designed based on psychological fundamentals that focused on colour and movements, as the user was provided with websites that contained different colours for the security intervention indicators. The results showed that most of the 29 participants focused longest on the red password field. In [3] the researchers analysed 214 U.S. financial websites for visible security design flaws. These flaws included: break in the chain of trust; presenting secure login options on insecure pages; having contact information on insecure pages; inadequate policies for users' passwords; emailing security information insecurely. Using an automated tool to analyse websites, the authors in [3] detected at least one visible security design flaw in 76% of the analysed websites.

The present study does not focus on improving the security warning indicator, nor does it examine the effectiveness of security indicators (as do the studies reviewed above). Rather, it examines users' behaviour and understanding in the context of the online-banking authentication process.

B. Security Warning in Online Banking

Banking websites generally attempt to apply advanced security features and requirements in order to attract users [1]. The potential for fraud may be higher in financial websites, and security warnings and indicators are therefore more prominent during their use. Few studies have focused on examining security warnings in a banking context. The authors in [7] enrolled 67 bank customers in a study that evaluated authentication measures and provided the users with several alarming clues, including removal of the 'https' indicator, removal of the security image and presentation of a warning message. The results from the study showed that the security image seems to be ineffective, as most of the users in different groups entered their passwords even when the security image was missing. Another study in [6] focused on the effectiveness of the security image by simulating a banking website and observing how 482 users interacted with the absence of a security image. The results showed that the majority of the subjects (73%) entered their passwords while the security image was absent.

Our study contributes to this research by capturing through empirical and realistic user study an understanding of users' awareness of visible security design flaws and security warnings in a banking context. In an explicit attempt to remedy a gap in the research, more security features are examined than have been in previous studies.

III. Methodology

A. Study Objectives

The goal of the current study was to examine users' awareness of security features by focusing on their behaviour and reactions to the security indicators. These features include the following:

- Working in an insecure page. Most financial websites use a secure encryption connection implemented via Secure Socket Layer (SSL); this is usually very clear to the user due to the presence of the 'https' and the lock icon in the address bar, indicating a secure connection to prevent hackers from attacking.
- Entering email information in an insecure page. The presence of an insecure page forces users to be more careful in sending and receiving information (such as email addresses).
- Responding to warning messages. The best way to examine a given user's awareness of security features and study his or her ability to read and decide is to provide the user with a warning message. One warning message that frequently appears on financial websites is 'invalid security certificate'. In this study, we provide the subjects with fake warning messages to examine their awareness and understanding.
- Providing biometrics information (finger print) on an insecure page. Biometrics information is considered highly sensitive and must be sent via secure, encrypted connection. The user's personality often ensures that his/her own sensitive data will be sent via secure connection.

Given the above items, the study was designed to answer the following questions:

1) To what extent are users aware of security indicators?
2) How do users behave in response to security features?
3) Did users with security experience behave cautiously with security features?

B. Study Design

Our study design was based on usability principles that

focused on ease of use, which is one of the main goals of human–computer interaction. Therefore, to obtain the most accurate results possible we aimed to provide a realistic experience in order to encourage users to behave as they do in the real world. A real online banking platform was simulated using the banking information (card and token) belonging to the first author of this paper. The system was programmed to simulate original online banking in the United Kingdom (HSBC). The simulated system required the user to register using an ID number, followed by creating and answering security questions and choosing a preferable physical method for using the site (card, secure device or finger reader). HSBC Bank originally used one method (a secure token); the security device used in this study is a device belonging to the researcher's account (first author of this paper) with HSBC Bank. The finger reader used in this study is SecuGen Hamster Plus, and the card reader belongs to the researcher's account (first author of this paper) with Barclays Bank. The other items used for the study include a consent form, scenario sheets and observation sheet.

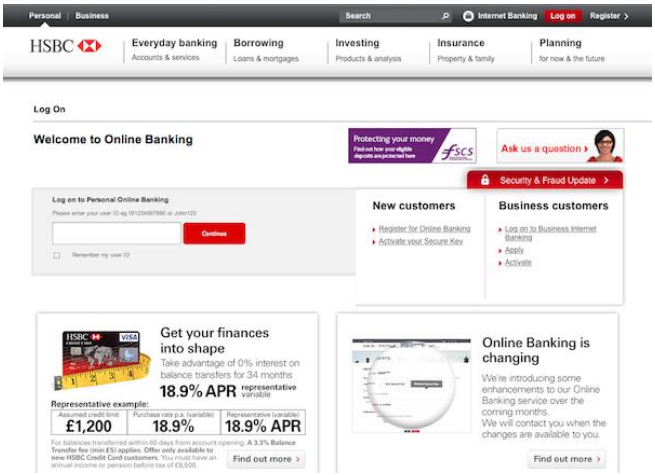

Fig. 1. Home Page for the simulated website.

C. Participants Recruitment

We recruited users by advertising the experiment in the main library of University of East Anglia; we offered a £5 honorarium for their participation. The participants were informed that they would perform a normal financial task using the banking information of the first author of this paper for research requirements. Participants were informed that no risks to their banking information existed as a result of their participation, and that access to their banking information or tools was not required.

D. Study Scenarios and Users' Tasks

The experiment was conducted in the main library of University of East Anglia. Each user was required at the beginning to sign a consent form; after signing, the user was provided with a detailed scenario of the task and required information. Participants started by logging in to HSBC Bank using the provided ID and the answer for the security question; the authentication process was completed using one of the provided methods. After the authorisation process, the participant executed a normal financial task that involved making a payment to a friend using the information provided in the scenario sheet. The following task required the participant to enter the provided email address in the scenario sheet to receive a confirmation receipt for the transfer process. Table I describes the experiment scenario.

TABLE I: EXPERIMENT'S STEPS

Step	Description
1	Enter ID number
2	Answer the secure question
3	Choose your preferable method for authentication
4	Complete confirming credentials
5	Press Proceed
6	Make a payment by filling all required fields
7	Click Continue
8	Confirm the payment process by entering email address
9	Retype the email address
10	Click Pay now

During the experiment, participants faced several security flaws, including: removal of 'https' in all address bars for the website pages of the simulated online HSBC Bank; a warning message indicating that the certificate verification is not trusted. The researchers' role was to observe participants' reaction to these flaws by monitoring participants' attention to the removal of 'https' from the address bars; providing the login information and email address; noticing the multiple methods provided for the authentication step; and completing the task. The database recorded users' responses to warning messages and time spent on each page. The bank database was a relational database designed and implemented using the MySQL relational database system.

After completing the experiment, we asked each participant to fill in a questionnaire to collect the demographic information and obtain the background experience.

IV. Results Analysis and Discussion

A. Respondents' Profile

One-hundred users (50 male and 50 female) participated in our experiment (Table II shows all demographic data). The participants had different nationalities, but the majority (78%) were British. Participants also reflected a broad range of ages, levels of education, and different college majors. All subjects had used the Internet for more than three years; based on this, we assumed our respondents had a high IT literacy level. Regarding the usage of online banking, 3% of our subjects had a banking account but had not previously used online banking, while (97%) had used online banking before. To provide more detail, 12 participants had used online banking for less than one year, 54 participants between one and three years and 31 for more than three years. In general, it is a positive finding that almost all of our subjects had some previous experience with online banking. We also ascertained that 40% of our subjects had an account with our simulated bank (HSBC Bank). In investigating whether subjects had experience in the domain of online security, we found that 12% of them had this experience, while 88% reported no experience. This allowed us to compare results between those who had experience and those who didn't, and observe their interactions more carefully.

TABLE II: DEMOGRAPHIC DATA

Gender	
Female	50
Male	50
Age	
18 – 25	65
26 – 30	10
31 – 35	20
Above 35	5
Education	
School	4
College	33
Undergraduate	48
Masters' Degree	10
PhD	5
Internet Usage	
More than three years	100
Online banking Usage	
Less than one year	12
One – three years	57
More than three years	31
Monthly usage of online banking	
0 – 3 times	34
4- 7 times	34
More than 7 times	31
Security Experience	
Yes	12
No	88

B. Absence of SSL and Lock Icon

During the experiment, all the pages were missing the Secure Socket Layer (SSL) and represented insecure connections; all the pages' links started with 'http' instead of 'https'. We observed users' progress during the login process, authentication process, and transaction process. By observing the users, we monitored for any hesitation or uncertainty concerning how to move from one page to another, complete the authentication process or provide all essential credentials. The results revealed that none of the 100 users participating in this experiment noticed that the 'https' was missing, indicating that the users had poor security experience, even those 12 users who indicated they had experience in the security domain. Moreover, none of the participants who held doctoral degrees, had taken classes in computer science/enrolled in school for computer science, or were enrolled in business school noticed the absence of the 'https' in the address bars.

C. Biometric Information (Fingerprints)

During the experiment, the second step was choosing an authentication method. One of the provided methods was the use of a fingerprint reader. For more clarification, the experiment's design aimed to force each user to use each authentication method during the experiment. For example if the user did not choose the fingerprint reader as an authentication method, he or she was asked to use it to confirm the transaction process. The observer ensured that the scanning stage passed easily and recorded users' reactions (such as confusion, hesitation, stopping, asking, and thinking). The results indicated that three out of 100 users wondered if their own fingerprints would be saved in the website database and asked the observer for more clarification. However, all of them completed the experiment after they obtained the answer to this question (two were from those in business school; one was from a participant enrolled in the development school). One participant expressed surprise after seeing his fingerprint on the screen and noted how fast the scanning process was. Most of the participants seemed to enjoy the experience of using the machine and scanning their fingerprint, and didn't express concern about the secure delivery of biometric information. Overall, it can be assumed that the participants do not have any experience in the domain of security and that they are not aware of the effects of their actions or decisions with respect to provision of fingerprints.

D. Invalid Security Certificate

During the transaction process represented in the experiment, a warning message regarding an invalid security certificate appeared. The user could choose to respond to this in one of two ways: press 'OK' or 'Cancel'. In order to record responses from users during the experiment, two methods have been used. First, the table schema was such that it recorded users' responses to the warning message options. The strategy used for capturing responses was that the expected response was set by default to FALSE(0) and updated to TRUE(1) when users selected creation option was selected. Second, the observer monitored and recorded users' responses to the message and all noticeable reactions recorded in the observation sheet. The results from the database indicate that 85 of the 100 users pressed 'OK' and proceeded to the next step; the remaining users pressed 'Cancel' to avoid the risk. Of the group defined as having some experience in the domain of security (a total of 12 users), only four pressed 'Cancel' with the other eight selecting 'OK'.

Table III presents details about user responses from the observation sheets collected after the experiment. The users' responses after the analysis are grouped by themes, with each theme describing one action as follows:

- Confused while reading the message and kept eye contact with the observer.
- Read the message very carefully, but careful reading did not lead to cancellation or stopping the set of actions related to continuing the online banking transaction represented by the experiment.
- Read the message and hesitated to proceed with the transaction.
- Asked for help from the observer.
- Indicated that they did not want to complete the experiment.
- Tried to find instructions.
- Read the message and press OK.
- Directly pressed 'OK' without evidently reading the message or expressing any concern.

Table III summarizes the above observations statistically. The majority of the users (68 %) did not spend time reading the message and responded directly (without reading it), while only 16 users read the message very carefully in order to make a decision. In spite of this careful reading, some of these users pressed 'OK', indicating they may not have understood the content of the message. Two of the users seemed to indicate that they were concerned about the account and desired to discontinue the task to avoid risk.

TABLE III: RESPONSES TO WARNING MESSAGE

Action	Frequency
Press OK	85
Press Cancel	15
From observation	
Confusing	1
Reading carefully	16
Hesitate to continue	7
Asking for help	5
Prefer to discontinue	2
Finding instructions	1
No concern	68

E. Providing Email Address

The last security feature examined in this experiment (and the last step in the task) was to provide an email address (which referred back to the researcher (firs author of this paper) in an insecure page. As such an email address is sensitive information that needed to be typed and transmitted on an insecure page in this experiment. It was assumed that some of the participants might have been aware of the risk. However, none of the participants hesitated or wondered whether they should stop participating during this step. Rather, all participants typed the email twice as requested without any concern. From this, it seems that an effort needs to be made by financial website providers to educate users with respect to the purpose of the security features. This study was performed with educated students from different levels who were very familiar with technology, but (as it turned out) didn't have the lowest level of understanding with respect to security features and dealing with risk. Providing users with online banking services without a security guide is inefficient. Therefore, we highly recommend that each user who opens an online banking account be compelled to read a mandatory page that shows all of the security requirements followed by simple and clear instructions on sending and receiving sensitive data prior to using the online banking platform. Future work will focus on a prototype of this recommendation.

V. CONCLUSION

The current study examined users' awareness and understanding of visible security features. The designed experiment for this study used a simulation of an actual online UK banking platform (HSBC Bank). One-hundred users were asked to perform a financial task that contained several security features. The findings of the study indicate that most of the users responded to the 'invalid security certificate' message in ways that showed they didn't realise the potential risk of their responses. Moreover, the results showed that none of the participants noticed the absence of the SSL connection used in common practice to secure website pages. To our knowledge, the study was also the first to examine users' responses to requests to provide biometric information on an insecure page. Only three of the 100 participants indicated concern related to the fingerprint request. In general, the study highlights the importance of educating online customers on security features as an essential part of online banking services. Future research will include other security indicators using different authentication methods.

REFERENCES

[1] M. M. Althobaiti and P. Mayhew, "Security and usability of authenticating process of online banking: User experience study," in *Proc. the 48 Annual IEEE International Carnahan Conference on Security Technology (ICCST '14)*, 13-16 Oct. 2014, Rome, pp 1-6.

[2] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Proc. the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems*, Florence, Italy ACM, pp. 1065-1074, 2008.

[3] L. Falk, A. Prakash, and K. Borders, "Analyzing websites for user-visible security design flaws," in *ACM SOUPS*, 2008, pp. 117–126.

[4] R. Kainda, I. Flechais, and A. W. Roscoe, "Security and usability: Analysis and evaluation," in *Proc. International Conference on ARES*, 2010, pp. 275–282.

[5] N. Kolb, S. Bartsch, M. Volkamer, and J. Vogt, "Capturing attention for warnings about insecure password Fields - Systematic development of a passive security intervention," *Human Aspects of Information Security, Privacy, and Trust*, Springer, 2014, pp. 172-182.

[6] L. B. Lee and M. L. Mazurek, "The effectiveness of security images in Internet banking," *IEEE Internet Computing*, vol. 19, no. 1, 2015.

[7] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The Emperor's New Security Indicators," in *Proc. IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 51-65.

[8] C. Seifert, I. Welch, and P. Komisarczuk, "Effectiveness of security by admonition: A case study security warnings in a web browser setting," *Secure Magazine*, pp. 1-9, 2006.

[9] D. Sharek, C. Swofford, and M. Wogalter, "Failure to Recognize Fake Internet Popup Warning Messages," in *Proc. the Human Factors and Ergonomics Society 52nd Annual Meeting*, 2008, pp. 557-580.

[10] D. Straub and R. Welke, "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly*, vol. 22, no. 4, pp. 441-469, 1998.

[11] S. Tuchscheerer, J. Dittmann, T. Hoppe, and J. F. Krems, "Theoretical analysis of security warnings in vehicles and design challenges for the evaluation of security warnings in virtual environments," in *Proc. the First International Workshop on Digital Engineering* Magdeburg, Germany, ACM, 2010, pp. 33-37.

[12] T. Whalen and K. M. Inkpen, "Gathering evidence: use of visual security cues in web browsers," in *Proc. Graphics Interface 2005*, Victoria, British Columbia Canadian Human-Computer Communications Society, ACM, 2005, pp. 137-144.

[13] M. S. Wogalter, "Purpose and scope of warnings," *Handbook of Warnings*, 2006, pp. 3-9.

[14] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proc. the SIGCHI Conference on Human Factors in Computing Systems*, Montreal, Quebec, Canada ACM, pp. 601-610.

Maha M. Althobaiti received the bachelor's degree with honors in computer science from Taif University, Saudi Arabia, and the master's degree in science from University of East Anglia with distinction and the highest mark within her class in Information Systems, United Kingdom in 2011. Currently she is working toward the PhD degree. Her research interests include security, usability, usable security, accessibility, e-learning and data mining.

Pam Mayhew left her job as a systems developer to study for an honors degree in computing and economics. She followed this with a PhD from the University of East Anglia that focused on Systems Prototyping. She now lectures at the same university in the systems analysis and systems engineering areas. She has published more than fifty papers including many on usability, e-commerce and m-commerce.