Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2009, vol. 14, no.1
(*http://www.arraydev.com/commerce/jibc/*)

Customers Perception of Security Indicators in Online Banking Sites in Nigeria

Egwali Annie Oghenerukeybe, D.M.E.
Lecturer, Faculty of Physical Sciences, University of Benin, Benin City. Nigeria
Postal Address: **Computer Department. Faculty of Physical Sciences. University of Benin. Nigeria.**
E-mail: egwali.annie@yahoo.com

Egwali Annie Oghenerukevbe is a lecturer in Faculty of Physical Sciences. University of Benin. Benin City. Nigeria. Her area of interests includes Information Technology, Software Engineering, Gender studies, E-commerce, Electronic Marketing and Software Security. To date, she has supervised several undergraduate and postgraduate students. She is currently carrying out analysis on issues relating to developing an enhanced Authentication Model into a Paperless Office Environment. She is a member of International Network for Women Engineers and Scientists (INWES), Nigerian Computer Society (NCS) and Third World Organizations of Women Scientists (TWOWS).

Abstract

Internet banking provides alternatives for faster delivery of banking services to a wider range of customers. The increasing popularity of Internet banking, have attracted the attention of both legitimate and illegitimate online banking practices. Customers are liable to criminal activities, fraud, thefts and various other threats of similar nature. Criminals focus on stealing user's online banking credentials because the username and password combination is relatively easy to acquire and then relatively easy to use to fraudulently access an Internet banking account and commit financial fraud. To alert users, many banking sites are now including Security Indicators (SI) to their sites. This paper describes a user study performed to investigate user's perception of factors influencing the effective implementation of existing SI objectives and to evaluate the effectiveness of SI in banking web browsers using the Communication-Human

Information Processing Model (C-HIP) model, a model proposed by Wogalter in 2006 in the field of warning sciences. Findings revealed that SI are not very effective at alerting and shielding users from revealing sensitive information to spoofed sites. These outcomes may help the management of banks develop effective security strategies for the future of electronic banking in Nigeria.

Keywords: **Security Indicators, Internet Banking, Warning Messages, User Study**

INTRODUCTION

The internet is the medium for an escalating amount of business and other sensitive transactions, including online banking and e-commerce. SSL/TLS is often used to protect traffic coming from and going to web applications. While this type of protection achieves the goal of data protection, unfortunately current browsers, still allows web spoofing, i.e. customers are tricked into revealing personal or financial information through a fraudulent website or e-mail message. The goal of attackers is often to obtain user-ID's, passwords/PINs and other personal and financial information, and abuse it e.g. for identity theft, larceny, or fraud.

As customers increasingly rely on the Internet for business, personal finance, and investment, Internet fraud becomes a greater threat. Internet fraud takes many forms, from phony items offered for sale to scams that promise customers great riches if assistance can be given to foreign financial transaction through the customer's own bank account. A common online phishing scam starts with an e-mail message that looks like an official notice from a trusted source, such as a bank, credit card company, or reputable online merchant. In the e-mail message, recipients are directed to a fraudulent website where they are asked to provide personal information, such as an account number or password.

A study by Anti-Phishing Working Group (2006), confirmed that about eight out of ten respondents have visited a spoofed web site and over 15% provided personal data to a spoofed site. Avivah (2004) conducted a user study and found that about two million users revealed sensitive information to spoofed web sites, and estimate a loss of about 1.2 billion$ to credit card issuers and U.S. banks in the year 2003. Aaron (2005) asserted that indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Spoofing attacks also causes substantial hardship for victimized consumers, due to the difficulty of repairing credit damaged by fraudulent activity. Both the frequency of spoofing attacks and their sophistication is increasing dramatically.

These demerits in Internet banking practices are really having a great impact in the adoption of Internet banking in Nigeria. As posited by Ezeoha (2005) Internet banking is slowly been embraced by customers because Internet practice in Nigeria has been abused by cyber attackers who use real and deceptive banking websites to scoop user's sensitive information and funds. If a deceptive spoofed site can be revealed as fraudulent to the intended customer, the attack can be thwarted. Thus customers are commonly advised by online security tips to pay attention to these indicators whenever they access a website. Unfortunately online Security Indicators (SI) have historically failed users because users do not understand or believe them.

The prevalence of spoofed sites has prompted the design of many new online SI. Because site spoofing is a semantic attack that relies on confusing customers, it is difficult to automatically detect these attacks with complete accuracy. Presently there are two types of SI tools used to alert or block users to probable spoof sites: Passive and Active SI. Passive SI indicates an impending danger by providing certain textual information, changing colors, or through other means without interrupting the user's online activity. Active warnings force the user to take notice of the warnings by interrupting the user's main online activity. However, research has shown that passive indicators are failing users because users often fail to notice them or do not trust them [Wu, 2006]. In this study both passive and active SI tools are referred to as SI.

The issue is that these SI do not actually prevent web spoofing attacks, Wu (2006) exposited that passive indicators are failing customers because customers often fail to notice them or do not trust them. Customers rarely pay attention to SI displayed in the peripheral area of the browser compared to the large main window that displays the web content at the right times to notice an attack. And sometimes SI make mistakes and identifies legitimate sites as spoofed sites, customers may learn to distrust the indicator. Then, when the indicator correctly identifies a spoofed site, the customer may not believe it.

The need for indebt knowledge of existing SI practices cannot be overemphasized. These warnings serve as the last defense against a user revealing sensitive information to attackers particularly during authentication into Internet banking sites.

This paper describes a user study performed to investigate users perception of factors influencing the effective implementation of existing SI objectives and to evaluate the effectiveness of SI in banking web browsers using the Communication-Human Information Processing Model (C-HIP) model, a model proposed in the field of warning sciences by researchers (Wogalter, 2006).

REVIEW OF LITERATURE

An emergent number of user studies are investigating why phishing attacks are so effective against computer users. Friedman et. al. (2002) in a surveyed analyzed concerns about the potential risks and harms of web usage on consumers and evaluated the web practices of 72 participants. It was discovered that consumers are really at risk. Fogg, et. al. (2002) conducted a number of large empirical studies on how consumers evaluate websites and developed guidelines for encouraging trustworthiness on websites.

Wu, et. al. (2006) carried out a user study to examine the effect of SI in preventing phishing attacks. In the study, users spend 34% of their time providing sensitive information to spoofed site even when toolbars were used to give notice of security concerns. Friedman et al. (2002) in an interview on web security showed four screen shots of a browser connecting to a website and asked participants to state if the connection was secure or not secure and to affirm the motivating factor for their appraisal. It was discovered that about 72 participants cannot tell if a connection is secure.

Whalen, et. al. (2005) used an eye-tracker to study user behavior with respect to browser SI and discovered that although subjects glanced at the lock icon in the status bar, however they hardly ever clicked on it. Sullivan (2004) conducted a web survey on how well users can distinguish phishing emails from legitimate ones. Screenshots of ten emails were shown to subjects and about 28% of the time, phishing emails was incorrectly identified as legitimate by the users. Ba et. al. (2002) carried out a pragmatic research in online trust which included a study of how manipulating merchant's feedback ratings can influence consumer trust in a merchant's site.

Jagatic, et. al. (2005) in a study on how successful phishing attacks have been, discovered that phishing attacks from trusted sites are more successful at compromising user's sensitive information than sites not trusted. In the study data was collected from the internet and used to create a social network map of university students. Faked phishing email from the map that appeared to be from friend's spoofed address succeeded in deceiving 72% of the responded while only 16% were deceived by spoofed sited from unknown addresses. A study by Jagatic (2005) established the fact that social context makes phishing attacks very far more successful. Phishing emails were sent to phishing sites that asked for the subject's university username and password, and validated them. About 72% subject's usernames and passwords were compromised.

Concerns for customers internet banking practices motivated some organizations to mount phishing attacks against their own members, with the goal of teaching them to protect themselves. Bank (2005) reported on how a US Military Academy at West Point found that more than 80% of its cadets succumbed to a phishing attack by a fictional colonel. Similarly the State of New York mounted two attacks on its 10,000 employees; 15% were spoofed by the first attack, but only 8% by the second, which came three months later.

Amer (2006) conducted a study to evaluate the motivational strength of software warnings. Participants were shown a series of dialog boxes with differing text and icons, and were instructed to estimate the severity of the warnings using a 10-point Likert scale. The researchers also examined the extent to which individuals will continue to pay attention to a warning after seeing it multiple times. Participant's choice in both icon and warning words greatly affected how each severity was ranked. It was discovered that users dismissed warnings without reading them after viewing them multiple times. This behavior continued even when using a similar but different warning in a different situation.

Chung, et. al. (2002) in a survey on the state of Internet banking in New Zealand confirmed the fact that security and complication of Internet banking are some of the factors limiting the full acceptance of Internet banking.

RESEARCH METHODOLOGY

Research Design

The intention of the study is to two-fold: to analyze user's perception of factors influencing the effective implementation of existing SI objectives and to evaluate the effectiveness of SI in these banking web browsers.

Thirteen banks in Nigeria were surveyed, representing 52% of the consolidated banks in Nigeria. The selection criteria were based on proximity of these banks within the southern part of the country and the availability of their online services. The study was conducted in the University of Benin, situated very close to where eleven branches of the banks are located. Users were informed to visit the online banking sites proposed for the study and attempt to perform normal online transaction. Users are later to fill in a post-task questionnaire on their online experiences.

The study commences with the use of a written survey that was designed to analyze user perception of SI and the effectiveness of SI. Participants were instructed to complete the questionnaires during class hours. The questionnaires are divided into three sections. The first section is for the profile of participants, the second section is to analyze users' perception of factors influencing the effective implementation of existing SI objectives while the third is to examine the effectiveness of SI in these banking web browsers using the Communication-Human Information Processing Model (C-HIP) model.

The first section includes participant's sex, age and banking practices (bank category, banking practice and bank location). The second section analyzes users' perception of factors influencing the effective implementation of existing SI objectives. Participants are to express themselves using seven factors: Time of popups, Indicator-type (passive/active), Choice of icon, Message contents, Display size, Background colour and Display position. The third section verified the effectiveness of SI included in online banking web browsers using a model similar to that proposed by Wogalter in 2006.

For the survey, questionnaires designed consisted of a 5 Likert scale point, 5 for strongly agree, 4 for agree, 3 for indifferent, 2 for disagree and 1 for strongly disagree. Many a time, it happened that the customers' were not clear about the terminologies used in the questionnaire but this matter was solved through detailed explanation and by one to one discussion. The instructions requested respondents to tick the response, which best describe their affirmation. Respondents were assured of the confidentiality of their responses and their names were not included on the questionnaire.

Response Rate

300 level students of Computer Science Department with basic web experiences and who were highly connected with internet services offered by banks were requested to complete the survey forms, which included series of questions to facilitate the categorizing of banking sites SI as being effective or ineffective. The questionnaires were distributed and completed during class hours. Out of the 200 questionnaires, a total of 137 questionnaires were selected for the purpose of analysis.

Data Analysis Method

Studies on the sample banks were conducted between February and March, 2008. For data analysis on users perception of factors influencing the effective implementation of existing SI objectives, tests for significant interactions amongst variables were performed using the classical chi-squared for independence of categorical data. The study also tested reliability of the instruments in order to produce a robust and valid result.

Finally, the study employed the Communication-Human Information Processing Model (C-HIP) similar to that proposed by Wogalter in 2006 to determine the effectiveness of SI in thirteen Internet banking web browsers.

Research Model

The effectiveness of SI in present online banking web browsers, particularly during customer's authentication phase, was analyzed using a model similar to that proposed by Wogalter in 2006. Wogalter (2006) proposed the Communication-Human Information Processing Model (C-HIP) designed for structuring warning research. The model assists in ascertaining if SI are effective or not. The model involves various phases for analyzing SI effectiveness. The various phases of the Communication-Human Information Processing Model (C-HIP) includes source, channel, delivery, attention switch, attention maintenance, comprehension memory, attitude and beliefs, motivation, behavior and environment stimuli. To analyze SI effectiveness as it relates to users internet banking practices, the model will be implemented from the *source* phase to the *environment stimuli* phase as these phases affects the user directly while authenticating into internet banking sites. The different phases as shown in figure 1 are:

Source: The source of the warning.
Channel: The channel through which the source warning appears.
Delivery: The delivering nature of the warning.
Attention Switch: The immediate attention capturing capacity of the SI.
Attention Maintenance: The degree at which Users attention capacity is maintained.
Comprehension Memory: Users knowledge of the purpose of the indicators and corresponding actions to take.
Attitude /Beliefs: Users trust of the intention of the indicators
Motivation: The incentive to take the recommended actions.
Behavior: The actually performance of the recommended actions.
Environment stimuli: The interaction of SI with other indicators and other stimuli.

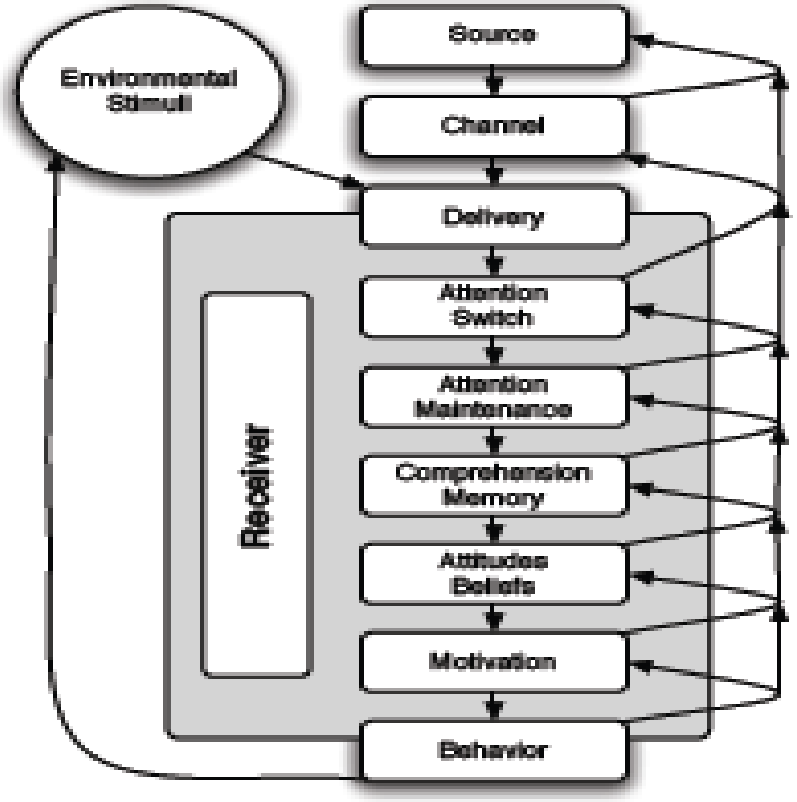

Figure 1. Communication-Human Information Processing Model (C-HIP). Source: Wogalter (2006)

RESULTS AND DISCUSSIONS

Correspondents Profile

		N = 137	**%**
Sex	Male	79	57.7
	Female	58	42.3
Age Range	18-20 years	53	38.7
	21-25 years	71	51.8
	26 – 35 years	13	9.5
Bank Category	First City Monument Bank	1	0.7
	Zenith Bank Plc.	9	6.6
	Unity Bank	12	8.8
	Union Bank	3	2.2
	United Bank of Africa	23	16.8
	Skye Bank	16	11.7
	Oceanic Bank	7	5.1
	Intercontinental Bank	27	19.7
	Guaranty Trust Bank	4	2.9
	Afribank	2	1.5
	Access Bank	11	8.0
	Diamond Bank	5	3.6
	First Bank Plc	17	12.4
Banking Practice	Offline only	82	59.8
	Online and Offline	55	40.2
Bank Location	Off Campus only	41	29.9
	On Campus only	27	19.7
	Off Campus and On Campus	69	50.4

Table 1: Profile of Respondents

Table 1 shows the profile of respondents. The respondents were made up of 79 males (57.7%) and 58 females (42.3%). The age ranged was between 18 – 20 years (38.7%), 21 – 25 years (51.8) and 26 – 35 years (9.5%). As their primary banking category, 1 respondent (0.7%) use First City Monument Bank, 9 (6.6%) use Zenith, 12 (8.8%) use Unity, 3 (2.2%) use Union, 23 (16.8%) use United Bank of Africa, 16 (11.7%) use Skye, 7 (5.1%) use Oceanic, 27 (19.7%) use Intercontinental, 4 (2.9%) use Guaranty Trust, 2 (1.5%) use Afribank, 11 (8.0%) use Access, 5 (3.65) reported using diamond, and 17 (12.4%) uses First Bank. In performing banking transaction, 82 participants (59.8%) carry out transaction offline only while 55 (40.2%) carry out both online and offline transactions. As their primary banking location, 41 correspondents (29.9%) carry out banking transaction outside the campus, 27 (19.7%) bank only in the campus, and 69 (50.5%) carry out banking transactions either on-campus or off-campus.

The second section analyzes the effectiveness of SI at alerting users by endeavoring to find out the SI perceptive level of customers, participants are to express themselves using seven factors: Time of popups, Indicator-type (passive/active), Choice of icon, Message Contents, Display size, Background colour and Display Position. The third section verified the effectiveness of SI included in online banking web browsers using a model similar to that proposed by Wogalter in 2006.

Users Perception of SI factors

S/N	**Statements**	**Strongly Agree**	**Agree**	**Indifferent**	**Disagree**	**Strongly Disagree**
1	Time of popups	27	24	16	2	9
2	Indicator-type (passive/active)	11	19	23	5	25
3	Choice of icon	21	21	16	7	21
4	Message Contents	16	18	22	11	12
5	Display size	11	27	11	6	17
6	Background colour	10	21	18	13	33
7	Display Position	13	7	20	9	6
	TOTAL	**109**	**137**	**127**	**53**	**123**
	MEAN	**15.6**	**19.6**	**18.1**	**7.6**	**17.6**

Table 2: Users perception of factors influencing the effective implementation of existing SI objectives.

From Table 2 the following can be extrapolated:

i. Respondents agreed to the fact that the time SI are popped up or displays to alert web users of the insecurity in using a site as much effect on the subsequent behavior of the user. It contributes to either being alert to obey the warning instructions on time or ignoring the warning altogether.

ii. Next is the choice of icon used for the SI display. Respondents consent to the fact that the choice of icon display has a lot of impact on the user subsequent behaviour to reduce vulnerability level.

iii. The least factor with any effect on users is the background colour used for displaying the SI.

X	O	E	(O –E)	$(O – E)^2$	$X^2 = \frac{(O – E)^2}{E}$
Strongly Agree	109	109.8	-0.8	0.64	0.006
Agree	137	109.8	27.2	739.84	6.74
Indifferent	127	109.8	17.2	295.84	2.69
Disagree	53	109.8	-56.8	3226.24	29.38
Strongly Disagree	123	109.8	13.2	174.24	1.59
TOTAL	**549**	**549**			**40.406**

Table 3: Chi-Square Analysis

From the Chi square analysis of the resultant data in table 2, the derived result (table 3) is significant beyond the 0.001 level ($p < 0.001$). This gives a 99 percent confidence that the differences between the observed and expected patterns of frequencies does not result from mere random variability.

Effectiveness of Internet Banking SI

C-HIP Phases	Statements	N = 137	%
Attention Switch	Never noticed the appearance of a passive SI	27	19.7%
	Noticed the appearance of a passive SI	110	80.3%
Attention Maintenance	Familiar with the different types of SI displayed	43	31.4%
	Read entire warning message	75	54.8%
	Aware of the consequences of not taking note of such warnings.	43	31.4%
	Saw warning and left site	13	9.5%
Warning Comprehension	Not understand the full meaning of the SI.	37	27%
	Comprehend that the sites were prone using spoofed sites to steal sensitive information.	11	8%
	Saw the SI revealed that they thought they were expected to log out of the banking sites immediately and discontinue the entering of sensitive information.	12	8.8%
	Saw warnings claimed to belief that they felt that their actions will results in the site being spoofed.	7	5.1%
Attitudes and Beliefs	Saw warnings but ignored them	19	13.9%
	Confused some of the warnings that appear alike.	23	16.8%
Motivation	Motivated to log out of the banking sites	19	13.9%
	Motivated to pay attention because the warnings made them believe they were about to be attacked.	21	15.3%
	Submitted information because they were unaware of the risks, used to ignoring similarly designed warnings or because they did not understand the choices that the warnings presented.	25	18.3%
Environmental Stimuli	Ignore SI and entered sensitive information because of trusting the site	18	13.1%

Table 4: Results of the effectiveness of Internet Banking SI based on the (C-HIP) model

Table 4 shows the results obtained from analyzing the effectiveness of Internet Banking SI (warnings) using the (C-HIP) model.

Attention Switch

At the “attention switch” phase, a warning will not be noticed on time if it is incapable of capturing user’s attention from the user’s present online activity. If it is incapable of capturing user’s attention on time to impose secured user behavior then it is ineffective.

For sites with passive warnings, 27 of the 137 participants never noticed that a warning appeared because their focus was either on the keyboard and they were ignorant of the fact that such messages exist and will be popup at that point in time. This finding is similar to those of earlier studies made by Zhang, et al., (2007). The timing for the appearance of the warning messages in 7 sites was about 8 seconds, thus a user who is ignorant of such warning messages can in the course of typing dismiss the warning. In the case of active warnings, 9 of the sites captured user's attention by interrupting user with a warning message; users are then left with the choice of continuing or exiting the current banking site. This type of warning succeeded because user's tasks were interrupted.

Attention Maintenance

For SI to be effective, then it must not only be able to capture user's attention but also be able to sustain the attention of users long enough for them to understand the significance of the SI.

43(31.4%) participants claim to be familiar with the different types of SI displayed in the different banking sites because they have seen them before and know what they denote. These same participants also claimed to have read the warnings because they were aware of the consequences of not taken note of such warnings. But it is likely that some users will not bother to read the full contents of warning messages even though some of these warnings are to some extent different and more severe. Thus it is very likely that if a message is recognized, users are less prone to reading such messages.

75(54.8%) participants claimed to have read the entire warning message that was displayed. 13(9.5%) participants said they left the site when the warning message was displayed because they felt that it was a spoofed site. In this case the SI did not protect the users but their ignorance did.

Warning Comprehension

An ingenious warning must be correctly understood, it must communicate a sense of danger and present suggested actions. Users do not need to completely read it to know the appropriate actions to take. Participants were asked what their understanding of each SI meant.

37 participants did not understand the full meaning of the SI. It was observed that 11 of the 110 participants who noticed the SI were able to comprehend that the sites were prone using spoofed sites to steal sensitive information. 12 of the participants who saw the SI revealed that they thought they were expected to log out of the banking sites immediately and discontinue the entering of sensitive information. While 7 participants who saw some of the warnings claimed to belief that they felt that their actions will results in the site being spoofed.

Attitudes and Beliefs

Well designed SI should be able to influence user's attitude and trust of the intention of the warnings depicted.

Participants were asked how their attitudes and beliefs influenced their SI perceptions and it was discovered that there is a significant correlation between believing the SI and allowing them to influence the attitudes of participants. The study revealed the fact that 19 (13.9%) participants ignored the warnings completely. A finding similar to that of Downs, et. al. (2006). (16.8%) participants confuse some of the warnings that appear alike. Thus gross warnings can be confused for minor ones if the warning formats are similar.

Motivation

An SI should be designed in such a way that it stimulates and effect the desired user behavior. The study revealed the fact that passive SI is less motivational than active SI.

19(13.9%) of the participants who saw the SI were motivated to log out of the banking sites, an action that although might seem good at the time but is liable to different approach. 21 of the 74 participants who saw the SI were motivated to pay attention because the warnings made them believe they were about to be attacked.

25(18.3%) participants who chose to submit information said that they did so because they were unaware of the risks (because they did not read the warnings), were used to ignoring similarly designed warnings (habituation), or because they did not understand the choices that the warnings presented.

Environmental Stimuli

Site confidence gained as a result of environmental stimuli.

18(13.1%) participants who ignored the warnings said they did so because they have absolute confidence in the sites. This finding is similar to those of Florencio, et. al. (2007) and Moore, et. al. (2007).

CONCLUSION

This study reveals the effectiveness of SI in Internet banking sites in some selected banks in Nigeria as it relates to users revealing sensitive information to spoofed sites. SI designed to alert users and to signal site trustworthiness were not fully comprehended by many participants. 37 (27%) participants did not understand the full meaning of the SI noticed in the banking sites while the attention of some users were not captured enough, for they ignored the warnings completely. Even with the presence of SI, 25(18.3%) participants still went ahead to submit sensitive information.

As spoofing attacks on user's sensitive information continue to advance, attackers success at compromising customers credentials will become rampant. While it has been suggested that SI be designed in such a way that they interrupt the user's primary task, clearly convey the recommended actions to take, fail in a secure manner if the user does not understand or ignores them, draw trust away from the suspected spoofed banking website, and prevent the user from becoming over familiar with the sites, a different approach is needed in order to adequately secure customers sensitive information in website during authentication particularly banking sites. The appearance of SI under trusted or mistrusted conditions is not enough. SI positioned outside the immediate eye range of users will continue to be ineffective or the use of passive SI.

An adequate solution must take into cognizance an enhance authentication procedure that is customers friendly and that will be secured even in an unsecured environment.

RECOMMENDATION

For Users of Internet Banking Sites

1. Caution should be taken when entering into banking sites in Nigeria. The location of the IS should be inspected. SI appearing as part of the web page should not be trusted.
2. Users of Internet banking facilities should use browsers with improved security and identification indicators. If possible indicators should be customized at significant sites.
3. Banking sites should be contacted by typing their address in the location bar, using a bookmark or following a link from a secure site, preferably protected by SSL/TLS.
4. Internet banking services should be instructed to limit online transactions in personal account to only what is really needed in order to restrict the damages due to spoofing.

For Owners of Internet Banking Sites

1. Shielded authentication operation that is not vulnerable to web spoofing should be employed in all banking sites in Nigeria. In particular, fingerprint authentication merged with the use of customized graphical models that employs the `challenge response` and one-time user authentication mechanisms would be effective against offline and online spoofing attacks.
2. SI should be designed to interrupt the user's task such that a user can continue transaction only after reading and implementing the required instruction. Active warnings are always more effective because they facilitated attention switch and maintenance.
3. SI should be designed to provide the user with clear options on how to proceed, rather than simply displaying a block of text.
4. The design pattern of less serious warnings should be different from that of more serious warnings so that users can be able to distinguish easily the difference and the urgency.
5. User's sensitive information should be transmitted using SSL/TLS.
6. Finally there should be constant educational programs organized for users to alert them on how to identify real sites from spoofed sites and how to always ensure secured online transaction.

References

Aaron, E. (2005). Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. Available at: http://www.dictionary.com/cgi-bin/dict.pl?term=radixlabs

Amer, T. S. and Maris, J. B. (2005). Signal words and signal icons in application control and information technology exception messages – hazard matching and habituation effects. Tech. Rep. Working Paper Series–06-05, Northern

Arizona University, Flagstaff, AZ, October 2006.

Anti-Phishing Working Group. Phishing Activity Trends Report, January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf

Avivah L. (2003). Phishing Attack Victims Likely Targets for Identity Theft, Gartner FirstTake, FT-22-8873, Gartner Research, 4 May 2004.

Ba, S. and Pavlov P. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, 26, 3 (2002), 243-268.

Bank, D. (2005). 'Spear Phishing' Tests Educate People About Online Scams. *The Wall Street Journal*. August 17, 2005.

Chung, W and Paynter, J (2002). An evaluation of Internet Banking in New Zealand. Proceedings of the 35th Hawarii international conference in system sciences. IEEE Hawarii, September 2002, pg 1-9.

Downs, J. S., Holbrook, M., and Cranor, L. (2006). Decision Strategies and Susceptibility to Phishing. In Proceedings of The 2006 Symposium on Usable Privacy and Security (Pittsburgh, PA, July 12-14, (2006).

Ezeoha, A.E (2006), Regulating Internet Banking in Nigeria, Problem and Challenges-Part 2. Journal of Internet Banking and Commerce, April, 2006, Vol. 11, No 1.

Florencio, D., and Herley, C. (2007). A large-scale study of web password habits. In WWW '07: Proceedings of the 16th international conference on World Wide Web (New York, NY, USA, (2007), ACM Press, pp. 657–666.

Fogg, B. J. (2002). Stanford Guidelines for Web Credibility. *Res. Sum. Stanford Persuasive Tech. Lab.*

Friedman, B. et al. (2002). Users' Conceptions of Risks and Harms on the Web: A Comparative Study. *Ext. Abs. CHI* (2002), 614-615.

Jagatic, T., Johnson N., & M. Jakobsson. (2005). *Phishing Attacks Using Social Networks* (*Indiana U. Human Subject Study 05-9892 & 05-9893)*.

Moore, T., and Clayton, R. (2007). An empirical analysis of the current state of phishing attack and defence. In Proceedings of the 2007 Workshop on the Economics of Information Security (WEIS2007) (May 2007). http://www.cl.cam.ac.uk/ twm29/weis07-phishing.pdf.

Sullivan B. (2004). Consumers still falling for phish. MSNBC. Available at: http://www.stargeek.com/item/212081.html

Whalen T. and Inkpen K.. (2005). Gathering Evidence: Use of Visual Security Cues in Web Browsing. In Graphics Interface. Available at:

http://portal.acm.org/ft_gateway.cfm?id=1089532&type=pdf&coll=GUIDE&dl=GUIDE&CFID=2824950&CFTOKEN=18618081

Wogalter, M. S. (2006). Communication-Human Information Processing (C-HIP) Model. In Handbook of Warnings, M. S. Wogalter, Ed. Lawrence Erlbaum Associates, pp. 51–61.

Wu, M., Miller, R. & Garfinkel, S. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Held in Montreal. ACM Press, pp. 601–610.

Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools. In Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS 2007) (28th February - 2nd March, 2007).