Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Examining Usage of Web Browser Security Indicators in e-banking: A Case Study

Thomas Nagunwa
Department of Computer Science, Institute of Finance Management,
Tanzania

Abstract - Over the last few years, many banks in Tanzania have taken an advantage of increasing internet penetration to deploy e-banking services. To guide and protect their security conscious customers from phishing attacks, banks are obliged to implement recommended web browser security indicators on their online banking web pages. These indicators also increases the trustworthiness of bank's websites thus ensure customers that they are interacting with genuine entities. This study examines the extent to which all 23 online banks in the country have implemented these security indicators on their online banking login web pages. Assessed security indicators include the use of HTTPS protocol, padlock, extended validation SSL certificate, URL characteristics, pop-up windows, security signs in web page contents and use of multi-factor authentication methods. The study concludes that no bank has implemented all indicators while a number of banks have failed to implement some of the key indicators. Certain banks use wrong security indicators. Local banks have done well in implementing most of the indicators relative to foreign banks. Banks are required to implement all indicators to increase trust and confidence to their online customers otherwise their online services will not be effectively used.

Keywords - E-banking, login page, phishing, browser, security indicator, bank, URL, online user credentials

I. INTRODUCTION

Over the last decade, Tanzania has experienced a rapid growth of a banking industry. From few banks in 1990s, now there are 34 commercial banks registered and regulated by the Bank of Tanzania (BOT)[1]. The country, in the same period, has undergone major developments in Information and Communication Technologies (ICTs) especially in internet availability, accessibility and its applications to organizations and individuals. From only 50,000 internet users in 2000 (penetration rate of 0.3%), now there are about 9.3 million internet users, 20% of the population [1], [2]. 50% of users access internet from their organizations, 45% from their households or personal devices while 5% get the access through internet cafes [3].

These developments opened doors to banks to widen accessibility of their services by establishing e-banking services. Today, 23 of the 34 banks are observed to provide e-banking services. E-banking[2] is the use of internet through which bank customers access banking services such as money transfers or bills payments. Customer use his/her login credentials mostly username and password to access bank account through a bank's website.

Banking industry is the second most targeted sector worldwide by phishing criminals, costing customers, banks and card issuers billions of dollars every year as total losses [4], [5]. One phishing attack in every 262 phishing attacks is targeting a financial sector [5]. Phishing is the stealing of online credentials such as bank account's username and password through different technological and social engineering skills to commit online fraud [6]. The most deployed phishing vector in the banking sector is spoofing of genuine banking websites which contributes to 69.8% of all phishing attacks in the sector [5].

As the e-banking sector in Tanzania is at infancy stage, it is less likely that the banks have well secured e-banking infrastructures and have well educated their customers on phishing. With the fact that many internet users in the country access internet through less secured or unsecured infrastructures such as internet cafes and household/personal devices, it is obvious that most e-banking users are at a high risk of phishing frauds. However, for customers with anti-phishing knowledge, banks have a responsibility of ensuring that they provide enough web browser security indicators for them to determine originality of the websites thus avoid visiting spoofed bank websites. If these indicators are not implemented, there is a chance that these customers assume e-banking websites they are visiting are not genuine and possibly are phishing websites therefore avoid using their online services. This in turn may lead to under-utilization of the costly e-banking resources.

This study aims at examining performance of the banks in implementing the indicators on their e-banking login pages. The e-banking login page of each bank providing e-banking services was examined to observe whether each indicator has been implemented or not. This study will help banks to assess their efforts towards alerting users on possible phishing

[1] http://www.bot-tz.org/
[2] http://www.investorwords.com/3420/online_banking.html

attacks and improve where they are not performing well. Bank customers will also benefit from this study by learning key indicators they should always look after, just before they login, to determine originality of bank websites.

The next section of the paper explains web browser security indicators used in this study. Section 3 describes related works while sections 4 to 7 explain the actual study. Section 8 concludes the paper.

II. WEB BROWSER SECURITY INDICATORS

Security researchers, experts and the Word Wide Web Consortium (W3C)[3] have proposed a number of features that can be used to differentiate genuine and secured websites from spoofed ones. These indicators are recommended to be used on web pages that are transacting user credentials and financial information. Bank customers conscious with phishing websites use these indicators to judge how genuine and secured the websites are thus affecting their decisions to use the online services. The indicators used in this study are explained below.

A. HTTPS Protocol

HTTPS is a HyperText Transport Protocol (HTTP) that uses Transport Layer Security (TLS) cryptographic protocol to secure its traffic [7], [8]. TLS, formerly known as Secure Sockets Layer (SSL), is incorporated in web browsers to ensure confidentiality, message integrity and entity authentication are achieved between client's browser and a server hosting the application [7], [9]. Confidentiality is attained through encryption of data from the sender using standard cryptographic algorithms such as Advanced Encryption Standard (AES) [7]. Message integrity means ensuring that a message sent by sender reaches to the receiver without any modification that could be performed along the way [7]. Entity authentication is the way a client use to confirm the originality of the server before establishing a communication [7].

Entity authentication is achieved through the use of SSL certificates. Certificate is a unique identity given to a business hosting an online service by a Certificate Authority (CA) after being approved as a genuine company and owner of the domain name [7], [9]. The certificate contains information including name of the company, its domain name, validity dates, unique public and private keys and the CA provided it [7].

When a client initiates a connection to the server, the client checks against the certificate of the server if, for instance, the company owns the accessed domain name, it a genuine business and its certificate is still valid [7], [9]. Once the check is passed successfully, the connection is established and data exchange is performed in encrypted form using the agreed encryption algorithm and public/private keys [7], [9].

A website or web page which is in a TLS-enabled HTTP connection with a server shows an indicator in a location bar of its URL beginning with *https* instead of *http* [7], [9]. For an e-banking website, it is expected that its login page's URL indicates *https* to inform users that all communications from submission of credentials and afterwards are TLS enabled.

The study observed if the banks' login page URLs start with *https*.

B. Padlock

An icon of closed padlock on the address bar is a key indicator for a TLS-secured HTTP web page [8], [9], [10]. Recent versions of all major web browsers including Internet Explorer, Firefox, Google Chrome and Safari show the icon on the address bar as a default location. Outside the address bar, the icon does not signify as an indicator [8], [9], [10].

In this study, we examined banks which have implemented the padlock at the address bar on their login pages.

Figure 1: Google chrome web browser showing https and closed padlock indicators on the address bar of a TLS-secured web page using SSL certificate.

C. Extended Validation SSL Certificate

Extended Validation SSL certificate (EV) is an improved SSL certificate required to be deployed by businesses to improve customers' confidence on their originalities. EV was designed in 2007 by CA/browser forum (CAB)[4], a voluntary group of CAs, web browser vendors and suppliers of applications using digital certificates. A key improvement in EV is that any entity requesting for a certificate must be approved by the CA according to the issuance guidelines provided by CAB [11], [12], [13]. The guidelines require CAs to;

- Verify legal identity as well as the operational and physical presence of website owner.
- Establish that the applicant is the domain name owner or has exclusive control over the domain name.
- Confirm the identity and authority of the individuals acting for the website owner, and that documents pertaining to legal obligations are signed by an authorized officer.

The guidelines also require CAs issuing the EVs to undergo EV auditing by a third party auditors recommended by CAB through audit programs such as WebTrust EV program audit [14]. Web browsers display enhanced indicators for EV on their address bars. These include name of the entity owns the certificate, change in color (green for address bar or URL

[3] http://www.w3.org/

[4] https://cabforum.org/

text if the certificate is valid) and a closed padlock icon [13], [15]. When entity's name is clicked, certificate information is displayed including name of the entity, domain name of the host, CA and certificate's period of validity. With EV, customers become more certain of the originality and existence of the online businesses they are interacting with.
The study examined how many banks use valid EVs.

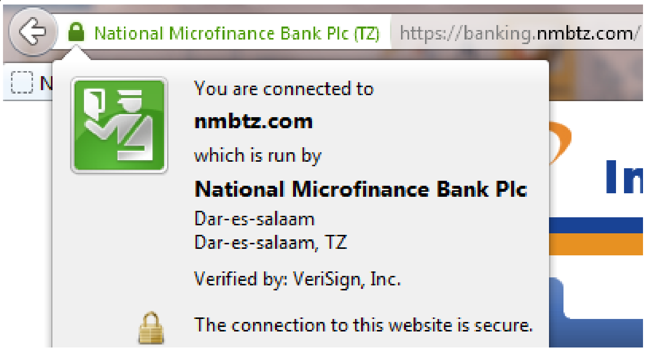

Figure 2: Firefox web browser showing EV indicators and EV certificate information.

D. URL Characteristics

1) URL and Domain Name Lengths

Long URLs are usually used by phishers to hide their suspicious components in them. A number of researches using comprehensive databases of phishing and non-phishing websites have concluded that URL and domain name lengths are among key differentiators of the two types of websites. [16] and [17] suggest that URL less than 75 long indicates a non-phishing site while above 75, the site is potentially a phishing one. In terms of domain name, length more than 30 characters is a phishing feature as suggested by [16].

2) Matching of Entity's Domain Name with URL's Domain and Certificate

[18] and [19] suggest that entity's registered domain name should match with the login page's fully qualified domain name (FQDN) and organization's name in the certificate. Completely mismatching may lead user to judge a website as a phishing one. SSL certificates do not show organization names therefore comparison of entity's domain name against organization names was only done to URLs with EV certificates. In this study, we categorized matching into *exact matching*, *close matching* and *not matching*. In exact matching, domain name of an entity exactly matches with the FQDN of the login page and organization name. Close matching refers to matching of large part of the domain name whereas not matching means they are completely different.

3) Non-IP based URL

To avoid their phishing sites being easily traced and shut down, phishers, in some cases, use IP addresses within their URLs in form of hexadecimal, octal or decimal numbers [7], [16], [18], [20]. URLs of genuine online businesses are expected not to use IP addresses.

4) Number of Dots in the Domain Name

Phishers tend to use fake multiple subdomains of hacked genuine domains to host their phishing sites, resulting in increased number of dots in the domain part of the URLs [20]. According to studies by [18] and [19], the average number of dots (in a complete URL excluding a path) is four or less for non-phishing URL while above four, the webpage is suspicious to phishing. We counted number of dots of domain part of each bank's login page and compared with the proposed threshold to determine if the bank has passed or failed to abide to this indicator.

5) URL Obfuscation Characters

Phishers use special characters to trick users into thinking that they are interacting with genuine URLs or directed to actual servers [7], [16]. Some characters are used to obfuscate host part of URLs while others in URL paths. Common characters are [- _ = ;] in the domain part and [@] in the paths [7], [16]. Non-standard ports can be used by phishers to divert traffic to phishing servers [16]. Standard port for https is 443, use of other ports may present a potential phishing attack. Non-phishing websites are not expected to use these characters or non-standard ports.

E. Security Signs in Web Page Contents

Some website designers use security signs such as closed padlock, TLS/SSL statements or CA logos in the content part of the web pages to present their trustworthiness [9], [10]. Studies have shown that users tend to depend on these signs to trust websites [9], [10]. Phishers can easily mimic these signs by design similar images in their spoofing sites leading users to trust their sites [10]. We examined if login page of each e-bank website has used these signs in its contents.

F. Pop-up Windows

Pop-up windows requesting user credentials are widely deployed by phishers to mimic original web pages to capture the credentials. A fake pop-up window can be inserted with an image of the true URL at the URL address bar, tricking users to think a genuine web page is being accessed [9]. Pop-up windows mimicking true web pages can also be placed on top or beside the true pages to capture user credentials [10]. Use of pop-up windows by e-banking web pages to prompt users for login credentials may raise suspicions of potential phishing attacks to customers and therefore not recommended for e-banking applications.

G. Multi-factor Authentication Methods
Singe-factor authentication method using ID/password has long been abused by phishers to hack online banks accounts [21], [22], [23]. Multi-factor authentication methods have since been recommended to financial institutions by security researchers, experts and authorities such as USA's Federal Financial Institutions Examination Council (FFIEC) and Council of European Professional Informatics Societies (CEPIS) to overcome weaknesses of single-factor methods [21], [22], [23]. The methods deploy at least two credentials to authenticate the user. Credentials may include password, PIN, one-time password (OTP), secret key, user selected picture, biometric characteristics, hardware tokens and others [21], [22].
Apart from improving security of user accounts, the use of the methods increases trust of the entity's site to its customers. As the methods are expensive to deploy and hard to spoof, phishing sites are unlikely to use them but banks are expected to implement them.
The study explored how many banks use multi-factor authentication methods.

III. RELATED WORKS
[9] did a related research in 2009 in which they assessed use of security indicators by top 125 websites. The websites comprised of 110 most popular domain names worldwide (by traffic), top ten banks in US, big four banks in UK and Australia, big five banks in Canada and top four American webmail providers. Only four indicators were used for this study compared to eleven indicators used in our study. The study showed that even websites of large companies such as Google failed to implement some basic security indicators.
[19] researched on to what extent the five largest Canadian banks implemented, on their websites, their own published security requirements including security indicators. In this study in which only two security indicators were used, results showed failure of some of the banks to implement one or both indicators.
Though indicators are insisted to be incorporated in sensitive websites, studies have shown that they are still not effective in preventing users from phishing attacks. A survey by [19] showed that most of security informed users do ignore most of the security recommendations by their banks including indicators. A study by [10] concluded that a significant number of online users do not know at all about security indicators while others use wrong indicators such as presence of CA's logos and padlock in website contents to determine originality of websites. Other users, even if are warned by the indicators about possible phishing attack, keep accessing the websites.

IV. OBJECTIVES
The purpose of the study was guided by the following key questions;
- What are the web security indicators recommended security experts and authorities?
- How each bank operating in Tanzania with online banking services has implemented security indicators?
- Are there any misuses of security indicators or use of wrong indicators?
- Are there differences in terms of performance in implementing the indicators between local and foreign banks?

V. STUDY DESIGN
A list of all registered commercial banks operating in Tanzania was obtained from the website of the bank registrar and regulator, BOT[5]. Non-banking financial institutions were not within the scope of the study. From the list of 34 banks, we accessed each bank's website, using website addresses we obtained from the same list, to determine which banks provide e-banking services.
23 banks were confirmed to have e-banking services working by accessing URLs of their login pages and testing, using dump credentials, to observe if the systems are responding and therefore know their activeness. We traced e-banking login pages through links from home pages of banks' websites and not by copying and pasting URLs. Nine of the 23 banks are local institutions while 14 are foreign institutions.
Since we had no user account to login to each e-bank site, we used login pages of these sites to measure the use of security indicators. Login page is significant in this study because it is where user gets a first impression of whether the e-banking website is safe or not and therefore decides to use the services or to quit. Phishers' interests are also to spoof login pages so as to steal credentials.
Security indicators were categorized into two groups, qualitative and quantitative. Each URL was assessed against each qualitative indicator and result recorded as *YES* if indicator was used and *NO* if was not. For quantitative indicator such as number of dots, the indicator was counted and then compared with the threshold. Final result then was recorded as *YES* or *NO* depending on the result of the comparison.
Current version of Google Chrome web browser was used to assess each bank's login page. Other web browsers were not used because their minor differences with Google Chrome in indicating some of the indicators would not have affected the results of the study.
Data was collected between November 13 and 27, 2013.

[5] https://www.bot-tz.org/BankingSupervision/registeredBanks.asp

VI. RESULTS

URL of each login web page was found to start with *https://* meaning that they deploy https protocol to secure transactions. Closed padlock was also observed in each web page, located in the address bar of the web browser.
12 banks (52%) use EV certificates while the remaining 11 banks (48%) use SSL certificates. 66.7% of local banks use EV while only 42.9% of foreign banks use EV.

Table 1:
Distribution of Local and Foreign Banks Using SSL And EV Certificates

Type of Certificate	No. of URLs	Local Banks	Foreign Banks	%
SSL	11	3	8	48
EV	12	6	6	52

Domain part of all URLs was found to be of less or equal to 30 characters. 17 of all URLs (74%) were found to be less or equals to 75 characters in length whereas six URLs (26%) were longer than 75, majority being foreign banks.

Table 2.
Distribution of Number of URLs against URL Lengths

Length	No. of URLs	Local Banks	Foreign Banks	%
<= 75	17	7	8	74
> 75	6	2	4	26

For matching between entity's domain name and login page's FQDN, 13% of all URLs had their FQDNs not matching completely with their entities' names. For instance, Bank of Africa (BOA) (T) bank has a registered domain of *boatanzania.com* but the FQDN of its login page's URL is *ebanking.bweb-portal.com*. The word *boa* does not even appear in the URL's domain. Similar cases observed to United Bank of Africa (UBA) (T) and FBME (T) banks. Coincidentally, all the banks failed in this indicator are foreign banks.
78.2% had a close match. For instance, National Microfinance Bank (NMB) uses *nmbtz.com* as a domain name but the FQDN of its login page's URL is *banking.nmbtz.com,* in which at least *nmbtz.com* appears in the URL. Only 8.8% managed to use exactly the same domain in their login pages.

All 12 banks using EV certificates had an exact match of the domain names with organization names in their certificates.

Table 3.
Matching of Banks' Domain Names and Login Pages' Domain Names

Match?	No. of URLs	Local Banks	Foreign Banks	%
Exact match	2	1	1	8.8
Close match	18	8	10	78.2
No match	3	0	3	13

All URLs were found not using IP addresses. None of the URLs was also found to have more than four dots in its domain part meaning that no redirecting domains or subdomains were used. One local bank, Exim (T), was observed to use @ in its URL path;
https://smartstatement.eximbank-tz.com/banking@homewebsource/Login.jsp
Three banks, Exim (T), BOA (T) and NIC (T), were found to use dash (–) in their URLs' domains;
https://ebanking.bweb-portal.com/EBKWebClient/login/start (BOA),
https://ebank.nic-bank.com/t24arcib1/servlet/BrowserServlet (NIC).
One foreign bank, Equity (T), used port number 446 for https protocol instead of 443, the standard port for https.

Table 4.
Use of URL Obfuscation Characters

Character	No. of URLs	Local Banks	Foreign Banks
@	1	1	0
-	3	1	2
Non-standard port	1	0	1

Eight banks (34.7%) were found to have security sign images in their web page contents, all of them having CA logos, mostly Norton's VeriSign. Half of the banks are local ones. Four banks (17.4%) were observed to use pop-up window designed login pages, three of them being foreign banks.

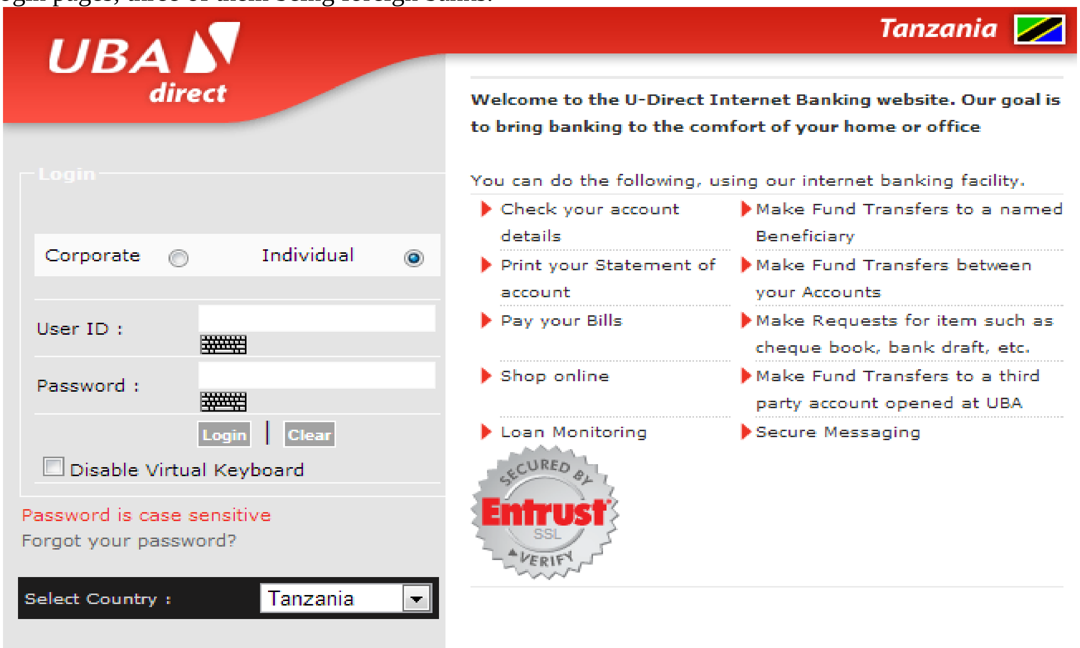

Figure 3: UBA's login page with an Entrust (CA) logo in the content part

Only eight banks use multi-factor authentication methods where four use one-time password, two use personalized pictures and the other two use PIN/key or secret number.

Table 5.
Multi-Factor Authentication Methods Deployed by Banks

Multi-factor method	**No. of URLs**	**Local Banks**	**Foreign Banks**	**%**
One-time password	4	2	2	17.4
Personalized picture	2	1	1	8.7
PIN/key/secret number	2	1	1	8.7

VII. DISCUSSION

By failing to implement some of the security indicators, it implicates that some of the banks operating in Tanzania are not aware of variety of phishing methods used today to spoof websites. Use of TLS secured channels with SSL certificates (by 48% of all banks) prevents man-in-the-middle attacks which is the not among the common phishing vectors today. Phishers can easily spoof https and closed padlock signs by replacing the address bar with its image containing the two indicators tricking users to think they are still in secured channels. This attack is noticed to be common to pop-up web pages, meaning that 17.4% of the banks using pop-up windows to ask for credentials are vulnerable to the attack. Compromising EV indicators is almost impossible therefore all banks were expected to deploy EV certificates.

Phishers can also compromise website hosts and create subdomains for their phishing sites. Un-matching of entity's domain name with that used in login page's URL as well large number of dots in the domain part should provide clues of possible attack of this nature. Phishers using their hosts to launch spoofed phishing sites can easily be exposed by the use of EV certificates. With this type of attack often accompanied with URL redirections and obfuscations, use of long URLs, obfuscation characters in domains and non-standard ports can play a significant role in raising suspicion of the attack. However, a significant number of banks have not implemented their respective indicators, as described in the results.

Use of CA's logos in login page's contents is not one of the security indicators as suggested by 34.7% of banks. This raises a concern that some of the banks do use wrong indicators with a confidence that they use the right ones. This may easily mislead their users to access spoofed sites with the same confidence of accessing genuine sites.

Majority of banks (65.2%) are still using single-factor authentication methods, suggesting that these banks either are not aware of vulnerabilities of these methods, avoid cost of deploying multi-factor methods or believe their customers use very strong passwords and they securely preserve them. As most of customers may be less knowledgeable on security, the later assumption may deceive the banks and thus risking their customers to hacking.

Generally, no bank was found to implement all indicators as per requirements. Phishers may study which indicators are missing from the sites and then launch attacks which cannot be avoided or indicated by the implemented indicators thus fooling even users who carefully look after the indicators. It is important that banks should implement all the indicators to cover a wide range of phishing clues.

The study shows that local banks are more aware of web security indicators against phishing compared to foreign banks. In majority of the indicators, local banks, though are few in number, have outperformed foreign banks. This is a surprising observation as there has been no phishing attacks reported against local financial institutions operating in the country, either originated within or outside the country. Contrarily, countries such as UK, India, Nigeria and South Africa, where most of the foreign banks are coming from, have a high number of reported online crimes. We therefore expected foreign banks, from their experiences to defend against online crimes, to take a leading role in all aspects of web security including the use of web security indicators.

VIII. CONCLUSION

Though no study is known to be done to learn the level of awareness of bank customers on phishing in the country, negligence on the use of web security indicators by the banks may affect maximum utilization of their online services. Customers with phishing knowledge may always depend on the availability of the indicators to make a judgment on whether to access the services or not.

Banks need to learn and deploy the right security indicators instead of implementing misleading ones such as security signs in web page contents. Banks may always fail a legal battle against their phishing victimized customers if they claim they followed misleading indicators.

Implementation of all indicators, with exceptions of EV certificate and multi-factor authentication, only need redesigning of website pages and URLs which are not costly at all. The other two indicators come with a small cost, which should be manageable by any bank institution.

Foreign banks especially those from countries with high phishing activities are expected to bring in their security experiences against phishing which can also be learnt by local banks.

Implementation of security indicators will be useless if banks' customers do not have significant knowledge about phishing. It is important that banks understand level of phishing awareness among their customers and then design specific awareness programs to inform them how to use these indicators, among other measures, to protect themselves against phishing. Without this approach, phishing attacks will always be successful against these institutions and their users, affecting users' confidence on e-banking and eventual collapse of the industry in the near future.

REFERENCES

[1] MiniWatts Marketing Group (2012), "Tanzania Internet Usage and Marketing Report", *Internet World Stats*. Available at: http://www.internetworldstats.com/af/tz.htm [Accessed November 2013].

[2] Mtweve, S. (2014), "Tanzania's internet users hit 9m", *The Citizen*. Available at: http://www.thecitizen.co.tz/Business/Tanzania-s-Internet-users-hit-9m/-/1840414/2254676/-/dgt0ps/-/index.html [Accessed April 2014].

[3] TCRA (2010), *Report on internet and data services in Tanzania – A supply side survey*, TCRA.

[4] McAfee Labs (2013), *McAfee Threats Report: First Quarter 2013*, McAfee.

[5] Symantec, (2013), *Symantec intelligence report July-2013*, Symantec.

[6] Anti-Phishing Working Group, (2012), *Phishing Activity Trends Report 4th Quarter 2012*, APWG.

[7] Nagunwa, T., (2008), *Investigation of data privacy threats in online retail industry and assessment used in mitigating their impact*, MSc Thesis, Dublin Institute of Technology.

[8] Roessler, T., Saldhana, A., (2010), "Web Security Context: User Interface Guidelines", *World Wide Web Consortium*. Available at: http://www.w3.org/TR/wsc-ui/#sec-tls-indicator [Accessed November 2013].

[9] Stebila, D., (2010), "Reinforcing bad behavior: The misuse of security indicators on popular websites", *Proceedings of the 22nd Conference of the Computer-Human Interaction*, pp. 248-251. Available at: ACM Digital Library [Accessed November 2013].

[10] Dhamija, R., Tygar, J., Hearst, M., (2006), "Why Phishing Works?", *Proceedings of the conference on Human factors in Computing Systems (CHI-2006)*, pp. 581-590. Available at: ACM Digital Library [Accessed November 2013].

[11] CAB, (n.d. b), "About EV SSL", CA/Browser Forum. Available at: https://cabforum.org/about-ev-ssl/ [Accessed November 2013].

[12] GoDaddy, (2013), "Premium extended validation SSL: Overview", Available at: http://www.godaddy.com/ssl/ssl-extended-validation.aspx [Accessed November 2013].

[13] Wikipedia, (2013), "Extended validation certificate", *Wikipedia*. Available at: http://en.wikipedia.org/wiki/Extended_Validation_Certificate [Accessed November 2013].

[14] CAB, (n.d. a), "Information for auditor and assessors", *CA/Browser Forum*. Available at: https://cabforum.org/information-for-auditors-and-assessors/ [Accessed November 2013].

[15] CAB, (n.d. c), "Information for site owners and administrators", *CA/Browser Forum*. Available at: https://cabforum.org/ [Accessed November 2013].

[16] Basnet, R., Sung, A., Liu, Q., (2011), "Rule-based phishing attack detection", *International Conference on Security and Management (SAM'11),* Las Vegas. Available at: http://weblidi.info.unlp.edu.ar/worldcomp2011-mirror/SAM8471.pdf [Accessed November 2013].

[17] McGrath, D., Gupta, M. (2008), "Behind phishing: An examination of phisher modi operandi", *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats,* article 4. Available at: ACM Digital Library [Accessed November 2013].

[18] Mohammad, R., McCluskey, T.L., Thabtah, F. A., (2012), "An Assessment of Features Related to Phishing Websites using an Automated Technique", *International Conference for Internet Technology and Secured Transactions (ICITST 2012),* pp. 492-497. Available at: IEEE [Accessed December 2013].

[19] Mannan, M., Oorschot, P.C., (2007), "Security and Usability: The gap in real-world online banking", *NSPW '07 Proceedings of the 2007 Workshop on New Security Paradigms*, pp. 1-14. Available at: ACM Digital Library [Accessed November 2013].

[20] Fette I., Sadeh, N., Tomasic, A., (2006), "Learning to Detect Phishing Emails", *WWW '07 Proceedings of the 16th international conference on World Wide Web,* pp. 649-656. Available at: ACM Digital Library [Accessed November 2013].

[21] Holbl, M., (2007), "Authentication approaches for online-banking", *Council of European Professional Informatics Societies (CEPIS).* Available at: http://www.cepis.org/files/cepis/20090901104203_Authentication%20approaches%20for%20.pdf [Accessed December 2013].

[22] FFIEC, (2005), "Authentication in an Internet Banking Environment", *Federal Financial Institutions Examination Council (FFIEC).* Available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf [Accessed December 2013].

[23] Owen, N., (2006), "Reducing Online Banking Fraud with Stronger Authentication Methods", *Bank Info Security*. Available at: http://www.bankinfosecurity.com/reducing-online-banking-fraud-stronger-authentication-methods-a-115/op-1 [Accessed November 2013].

