The urgent need for an enforced awareness programme to create internet security awareness in Nigeria

The Urgent Need for an Enforced Awareness Programme to Create Internet Security Awareness in Nigeria

Tiwalade Adelola
Department of Computer Science
Loughborough University
Loughborough, UK
t.adelola@lboro.ac.uk

Ray Dawson
Department of Computer Science
Loughborough University
Loughborough, UK
r.j.dawson@lboro.ac.uk

Firat Batmaz
Department of Computer Science
Loughborough University
Loughborough, UK
f.batmaz@lboro.ac.uk

ABSTRACT

Although the Internet offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users may not be aware of the dangers. As such, various countries have developed and implemented cyber-security awareness measures to counter this. However, there is currently a definite lack in this regard in Nigeria, as there are currently, little government-led and sponsored Internet security awareness initiatives. Also, a security illiterate person will not know of the need to search for these awareness programmes online, particularly in Nigeria's case where personal information security may not be an overly important issue for citizens. This paper therefore, is to establish the need for an enforced Internet security awareness programme for Nigeria that would assist in creating a cyber-secure culture in Nigeria among all of the users of the Internet.

Categories and Subject Descriptors

K.4.4 **[Electronic Commerce]:** Security

General Terms

Human Factors, Security

Keywords

Internet Security Awareness, E-commerce, Nigeria,

iiWAS '15, December 11-13, 2015, Brussels, Belgium
© 2015 ACM. ISBN 978-1-4503-3491-4/15/12…$15.00
DOI: http://dx.doi.org/10.1145/2837185.2837237

1. INTRODUCTION

Various studies have stated that privacy security is one of the main concerns for successful e-commerce implementation [1, 2]. The Internet enables people to share their personal information, but Internet users are prone to security attacks. These activities have raised the concern as to the security of the information being transferred, especially when it involves personal details such as real name, credit card details and bank account details. This also means that ignoring and not addressing the human issues of security through proper awareness initiatives and solutions would lead to these security issues not being addressed.

Most customers feel that security is solely the responsibility of a third party, for instance, the government, websites, banks, or IT professionals [6]. People need to be educated about information security so that they can protect themselves from these security threats. Existing research confirms the security concern about e-commerce in Nigeria, due to a general lack of awareness of cyber threats and an increase of online retail stores and e-commerce activity [7]. This paper primary focuses on Nigerian Internet home-users and the lack of Internet security awareness and suggests the need for enforcing Internet security awareness.

According to a Nigerian cyber threat survey [7], although cybercrime is common in Africa, it is more prevalent in Nigeria due to the population size, the push towards a cashless society, relatively high Internet penetration, lack of adequate security controls, and weak governance. It was also noted that many Nigerians are unskilled, which could pose a significant risk to the state of Internet security in the country. Slow e-commerce growth and increased mistrust are some of the consequences associated with cybercrime.

The next section will discuss related studies and concepts in Internet security awareness.

2. RELATED STUDIES AND UNDERLYING CONCEPTS

An Internet security awareness programme should aim to inspire, stimulate, establish and rebuild security and privacy skills and expected security practice from specific audiences. This is to reinforce good security practices by allowing individuals to recognise privacy concerns and respond accordingly [8]. The future of electronic commerce depends on enhancing consumers' security perceptions and maintaining the balance between perceived trust and online security.

2.1 Type of Audiences

There are many ways or domains to classify the different personal Internet users. Kritzinger and Von Solms [6] classify personal Internet users into two categories: Home Users (HUs) and Non Home Users (NHUs).

1. Non Home Users (NHU): NHUs are those users accessing the Internet from their corporate workplaces within their work environments. NHUs are often exposed to compulsory security awareness courses and will be governed by policies, procedures, guidelines and best practices to complete such awareness courses and perform secure practices when accessing the Internet.

2. Home users (HU): A definition of a HU is a citizen of any age and technical knowledge who accesses the Internet for personal use anywhere outside their place of work. Home users can be further divided into students, parents and educators, young professionals and older citizens;

The awareness programme described in this paper will focus mainly on Nigerian home users. This is because non-home users could have compulsory awareness training within their work environment unlike home-users who make use of the Internet without any training.

2.2 Common current training and awareness techniques

Training and awareness is generally accomplished using one or a combination of several techniques described below.

1**. Formal Training Sessions** represent the traditional approach to user training and awareness [9]. It could be in form of a video, in person training or specialised online training. This type of programme is usually organised by private sector organisations and government bodies [6].

2. **Passive computer-based and web-based training** represents a centralised approach to the training and awareness problem. An example is the website "Be Cyber Streetwise" whose aim is to ensure the online safety behaviour and confidence of consumers and small businesses improve [6]. There are a number of government-sponsored sites with tips, newsletters, resources and even videos for home users and small businesses

3. **Strategic placement of awareness messages** can raise the level of awareness through the delivery of the message by methods such as posters in public places, email messages, and media (TV adverts, newspapers) [9].

4. **Interactive computer-based training,** such as video games, can be used to improve security behaviour and awareness [10]. This approach can offer training and education for a range of target audiences from young school pupils to experienced IT personnel or even elderly citizens [6].

Figure 1 shows the components of an awareness programme. It displays the different types of Internet users, the various methods used to provide Internet security awareness and the organisations that provide the awareness programmes.

3. INTERNET SECURITY AWARENESS INITIATIVES

3.1 Developed Countries

To explore the way other countries promote Internet security awareness, a comparative analysis of two developed countries was conducted. From this analysis, the principal factors were determined and compared with the awareness situation in Nigeria in order to form the basis of the envisioned awareness programme. The countries analysed were the United States of America (US) and the United Kingdom (UK). These countries were selected due to their national cyber-security approaches and their membership of the Organization for Economic Co-operation and Development (OECD) [11]. The OECD is relevant because they provide guidelines for online practices.

In the US, the goal of cyber-security awareness and education is to raise the level of awareness in the nation of the risks of cyberspace, and how to avoid these risks [12]. A national organisation, The National Initiative for Cyber-Security Education (NICE), is dedicated to cyber-security awareness and education. NICE was created from a combination of governmental departments. In the UK, the goal is to support individuals and businesses by informing and educating them on the issue of cyber-security [13].Cyber-security awareness and education have been delegated to an external organisation, "Get Safe Online". The NICE Strategic Plan uses campaigns such as "Stop. Think. Connect" to equip the US public with the necessary knowledge and skills. The"Stop.Think.Connect" website [28] provides Internet security tips for different type of US citizens (parents, citizens etc.) and campaigns for different Internet security issues. The UK "Get Safe Online" website also has similar campaigns and tips tailored for different UK audiences. In these countries, it is obvious that the cyber-security awareness and education goal is run by the government or delegated to one or more departments or organisations to carry out.

3.2 Nigeria

Even though Internet access has yet to reach more than 50% of Africans, the continent's connectivity levels are nonetheless growing at a rapid rate. Data compiled by Internet Live stats 2015 [14] show that the African country with the highest number of Internet users in 2014 was Nigeria with 67.1 million users. The high figures of Internet usage and penetration in Africa have led to the awareness of cyber security threats and, as a result, countries have started to take steps towards improving their respective security stance [7]

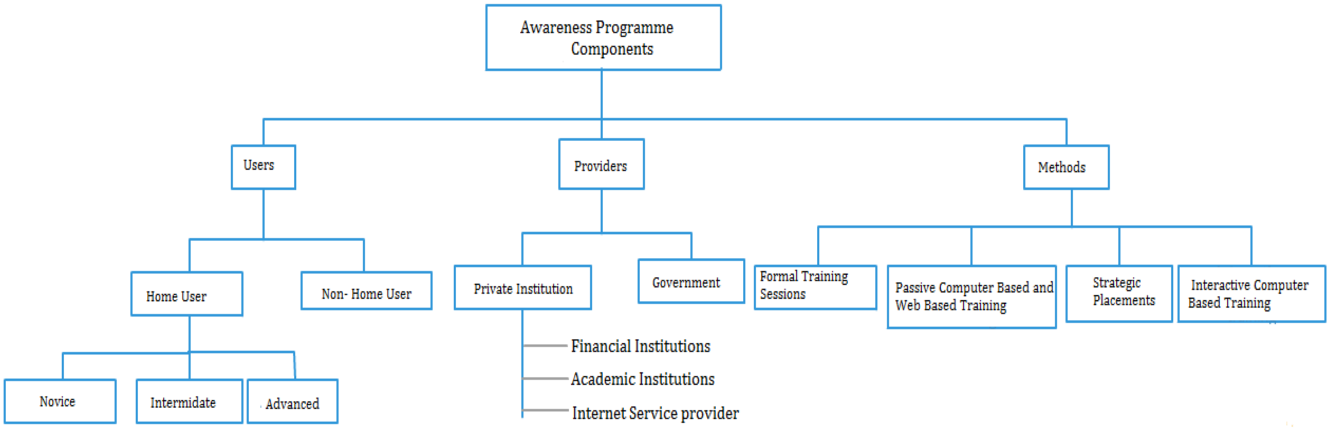


Figure 1. Awareness Programmes

While there is high internet penetration in Nigeria, the internet security culture is lacking. Nigerians are largely unaware of self-protection techniques and they show little concern for security issues. Also, the current awareness initiatives may be ineffective in combating these problems. This could pose be a major problem in the development of e-commerce due to Nigeria's high cybercrime rate.

This section of the paper will outline how African countries, and Nigeria in particular, are still lagging behind other countries in terms of establishing legislation and methods to deal with Internet security and creating initiatives to develop awareness about the dangers of the Internet. It will also outline Nigeria's unique factors that will justify the recommendation of an awareness programme that is different from the generic approach used in most countries. Most countries make use of online awareness websites and campaigns, which provide information on different Internet security issues.

3.2.1 Nigerians Perception of Privacy and Internet Security

Perceptions describe the ability and view of a person regarding a particular phenomenon [15]. A study was carried out to determine the public's understanding and knowledge of data protection and privacy in Nigeria [16]. 72 Nigerian Internet users completed a survey. The focus was on younger and educated Nigerians. The main reason for this is that, based on previous studies, the majorities of those who regularly use the Internet are within the age of 15-24 and have post-secondary education [7] and may well have different views on and approaches to the disclosure of personal information compared to those who rarely use the Internet. The research showed that 44% of the respondents were always or very often concerned about the use of their personal information and 58% of the respondents indicated concern about their information being used by third party websites. Ironically, more than a third was not aware of any self-protection techniques. These results show that there are concerns about Internet privacy and security, but the awareness about how to prevent issues is relatively lacking. This means that although the survey participants imply concern for security of their personal information, the lack of security awareness and knowledge shows there is actually no concern for these issues. A concerned Internet user would consciously look for information on how to protect themselves when online.

3.2.2 Current Initiatives in Nigeria

CSEAN (Cyber Security Experts Association of Nigeria) is a non-profit organisation whose aim is to expand the Nigerians' knowledge, awareness and understanding of the issues around cyber-crime and Internet security mainly through workshops and seminars [17]. The Cyber Security Experts Association of Nigeria (CSEAN) are partnered with "Stop. Think. Connect" a global cyber security awareness campaign. CSEAN will start the "Stop. Think. Connect" campaign in all tertiary institutions in Nigeria in the form of seminars [18].

ngCert (Nigerian Computer Emergency Response Team) is the national computer emergency response team that was created as a result of the 2015 Nigerian cybercrime bill [19]. Their website provides information on how to report a cybercrime incident. Most importantly, it provides some links to external advice and alerts on Internet security.

Although CSEAN has seminars and events to improve general awareness in Nigeria, they mainly use seminars to provide awareness. Seminars are not easily accessible to many people as they are location-restricted and usually costly to attend. The ngCert website fails to provide adequate awareness information on safe Internet practices as compared to other similar websites. For example, a similar UK website, the ICO (Information Commissioner's Office), provides advice on personal information protection and general Internet security [20]. There are a few links on the ngCert website to external resources but these are not informative enough.

4. AWARENESS PROGRAMME IN NIGERIA: ENFORCING INTERNET SECURITY AWARENESS

With growing numbers of Nigerian home users accessing the Internet, the big problem and worry is that, in many cases, such users are not information security aware, and are therefore potentially exposing themselves to attack [7]. Kritzinger and von Solms [6] suggested a way to force home users to gain necessary awareness before gaining access to the Internet. They pointed out that, unlike non-home users (NHU) who are probably exposed to compulsory security awareness courses and are governed by corporate policies, procedures, and guidelines when accessing the Internet, home users (HU) are not necessarily forced to obtain information security knowledge in any form. If HUs lack the proper information security awareness knowledge, they will also not understand and/or be aware of the cyber risks [4]. Figure 2 describes Kritzinger and von Solms's suggestion for enforced awareness before going online.

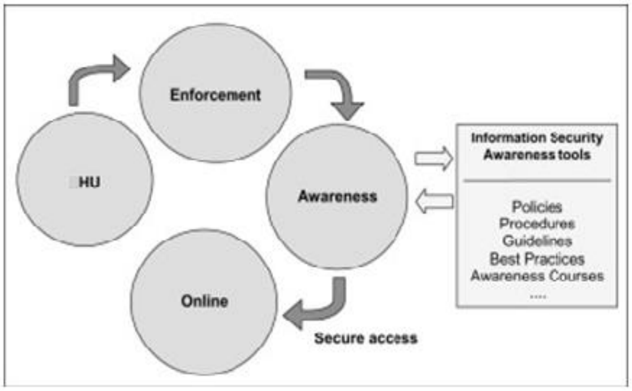


Figure 2. Compulsory secured access to the web for Internet users [6]

Although Nigeria has the greatest Internet penetration in Africa, many of its citizens are not aware of the dangers of the Internet [7]. Furthermore, Nigeria is one the top ten countries that contain the world's 775 million illiterate adults, with just 59.6% of the population above 15 years who can read and write [21]. The most common awareness programmes are web based. These programmes are, in most cases, not easy to find and with the low literacy levels in Nigeria, HUs may not have the skills and knowledge to find these programmes. If these programmes are found, they are, in most cases, not comprehensive enough, and do not include all relevant security issues [6], and furthermore, a security illiterate person will not know of the need to search for these awareness programmes online, particularly as personal information security may not be an overly important issue for Nigerians [22, 23]. From the discussion above, it is concluded that an awareness programme should be able to perform the following functions:

- Assess the literacy of the users and deliver the security awareness topics to the users based on their literacy level.
- Check if users' Internet security knowledge has improved since using the programme, thereby quantifying its effectiveness.
- Expose users to awareness tools to prepare them for the possible risks before obtaining access to the web.

4.1 Developing the Awareness programme

The National Institute of Standards and Technology (NIST) developed a framework that aims to guide the development of an Information Technology (IT) security programme [24]. This paper identifies the urgent need for an enforced awareness programme to create Internet security awareness among Nigerians. The NIST framework provides the steps that will be used to develop the awareness programme

1. Designing the Awareness Programme

To design an awareness programme, it is important to understand the current security issues that will help shape the strategy and design of the security awareness programme. This will identify the threats particular to Nigeria by examining the literature on current Internet security issues in Nigeria and observing and identifying the threats found in practice.

2. Developing Awareness Material

The issues to consider when developing awareness material are the selection of the awareness topics, and the sources of material for developing the awareness. This will be dependent on the issues discovered in the initial stage. An important aspect of an awareness programme is to ensure that information is appropriately tailored for target audiences. The home users should be grouped according to their Internet security knowledge such as novice, intermediate and advanced. This information could be obtained from a brief questionnaire in the programme. Different materials should be developed for each audience's needs, knowledge, and ability level. This is unlike the suggested awareness programme by Kritzinger and von Solms (2010), which uses a scalable system. This means that a user can start with introductory material and then move on to more advanced terminology. Each level will have a testing environment where the HU can be evaluated regarding the material of each level. A compulsory test might be cumbersome; a brief questionnaire will help to tailor initial content to the needs of the users and their current knowledge.

3. Implementing the Awareness programme

To implement the awareness programme, a selection should be made of the techniques through which the messages will be delivered. The different means of transferring security knowledge are through the use of formal training sessions, strategic placement of awareness messages, and passive computer-based, web-based, and interactive computer based training [6]. During the implementation of the awareness programme, a decision will need to be taken with regards to the delivery method. The chosen techniques will depend upon resources and the complexity of the messages. Another important aspect is to determine which organisation will implement the programme. A number of prospective organisations need to be considered based on their importance and applicability in the cyber security scene. Possible organisations to implement an awareness programme are:

I. **Governments** usually organise cyber security awareness programmes for the citizens to encourage good online practices. It usually involves online resources in the form of resource websites and campaigns in the form of posters and advertisements [19].

II. **Internet service providers (ISP)** provide awareness for their customers on Internet security issues and how they can manage them. They assist customers to protect themselves from online threats, e.g. with anti-virus and anti-spam software [25] In the case of Nigeria, telecommunication companies are also major Internet service providers. This type of enforced awareness programme can be implemented by the ISPs to educate their customers before they use their services. This could potentially protect their customers from potential dangers online and, at the same time, reduce strain on their services due to unwanted traffic on their network.

III. **Academic institutions** educate young people to use the Internet securely and safely. This is usually in the form of outreach and awareness programmes organised by internal and external security professionals [26]. Another method is to integrate the Internet security resources into the school curriculum to equip students with practical cyber safety skills and knowledge [27]. A number of universities now recommend providing security awareness training and education components for students and staff.

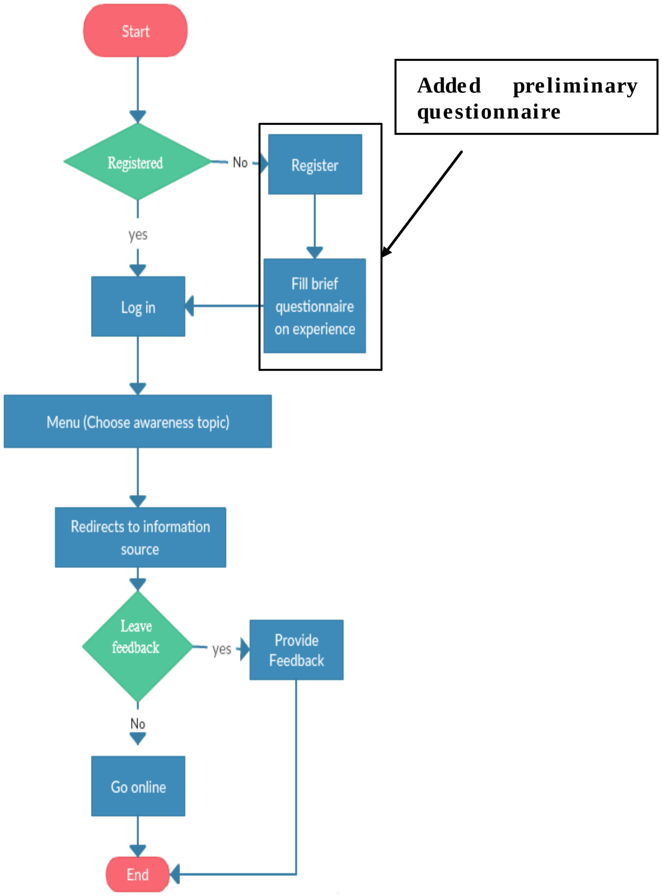
IV. **Financial Institutions** provide awareness for their customers on Internet banking security issues on their website, emails and newsletters. This could potentially reduce identity theft and fraud issues and, at the same time, improve their overall services to their customers

V. **Non-Profit Organisations** organise awareness campaigns whose aim is to expand the knowledge, awareness and understanding of the issues around Cyber-crime [17]. Governments usually delegate awareness programmes to such organisations.

4. Post Implementation

The final step of the NIST framework is Post-Implementation. Once the programme has been implemented, processes must be put in place to monitor compliance and effectiveness. The feedback provides a strategy to ensure that the programme continues to be relevant and compliant with the overall objectives. Assessments after the awareness programme can be used to determine if any knowledge has been effectively acquired and how it can be improved.

The flowchart in Figure 3 shows the suggested awareness programme discussed above.


Start
Registered
No
Register
yes
Fill brief questionnaire on experience
Log in
Menu (Choose awareness topic)
Redirects to information source
Leave feedback
yes
Provide Feedback
No
Go online
End

Added preliminary questionnaire

Figure 1. Awareness programme flowchart

This programme would be more effective if regulated by a non-government organisation whose provision of good services relies on the awareness of its customers. This is because even though an organisation, for example a bank, uses the best technical solution to provide adequate security, without the perception and awareness from customers these solutions may not be useful. An effective government could also regulate the programme. In the case of Nigeria, the government may not be currently effective enough to solely regulate this programme because of its known ineffectiveness and other priorities a developing nation would have [21]. The programme described above should make sure Nigerians are regularly exposed to Internet security content, which, in turn, will improve the views on the importance of personal information protection, improve Internet literacy and the general cyber-secure culture in Nigeria

5. FUTURE WORK AND CONCLUSION

Accessing the web has many risks for the home users who have limited Internet security knowledge. It is therefore essential to ensure that users are educated and understand the risks involved and how to limit them. In the case of Nigeria where there is a significant lack of awareness and absence of regulatory body, an awareness programme should empower users by giving them a better understanding of security issues, possible threats and how to avoid them. However, it is not enough to just provide an awareness programme, it is also important for citizens to easily find and make use of these awareness resources. The inclusion of a brief questionnaire into the programme will tailor contents based on the user's current knowledge and needs to ensure its effectiveness. This paper suggests that making use of an enforced awareness programme will not only provide an Internet security awareness programme, but also ensure it is being used effectively. Promoting a good Internet security culture will make online customers aware of websites, which make use of good security procedures and policies and those that don't. Future research could focus on effective ways to develop cyber-secure culture among the young population through school competitions and workshops on improving awareness, posters and social media. It is also important to research the applicability of these approaches in other developing nations with similar cyber-security and awareness issues.

A further step would be to concentrate on actually implementing the awareness programme in terms of a prototype to see its effectiveness. Surveys should be conducted with potential users and providers to determine the effectiveness and applicability of the programme.

6. REFERENCES

[1] Adkinson, W.F., Eisenach, J.A. and Lenard, T.M., 2002. Privacy online: A report on the information practices and policies of commercial web sites. Progress and Freedom Foundation, Washington DC.

[2] Antón, A., Earp, J.B. and Reese, A., 2002. Analyzing website privacy requirements using a privacy goal taxonomy, Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on 2002, IEEE, pp. 23-31.

[3] Symantec Norton, 2012. Norton Cybercrime Report," 2012.

[4] Furnell, S., Tsaganidi, V. and Phippen, A., 2008. Security beliefs and barriers for novice Internet users. Computers & Security, 27(7), pp. 235-240.

[5] Kritzinger, E. and Smith, E., 2008. Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5), pp. 224-231.

[6] Kritzinger, E. and von Solms, S.H., 2010. Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 29(8), pp. 840-847.

[7] Wolf Park and Digital Jewels, 2014. The Nigerian Cyber threat barometer report.

[8] Dlamini, I., Taute, B. and Radebe, J., 2011. Framework for an African policy towards creating cyber security awareness.

[9] Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D., 2007. A video game for cyber security training and awareness. Computers & Security, 26(1), pp. 63-72.

[10] Blythe, J.M. and Coventry, L., 2012. Cyber security games: a new line of risk. Entertainment Computing-ICEC 2012. Springer, pp. 600-603.

[11] Kortjan, N. and Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 52, pp. 29-41.

[12] National Initiative for Cybersecurity Education, 2015-last update, The National Initiative for Cybersecurity Education (NICE). Available: http://csrc.nist.gov/nice/awareness.html [8/20/2015, 2015].

[13] UK Government Cabinet Office, 2013-last update, Protecting and promoting the UK in a digital world: 2 years on. Available: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world-2-years-on [08/20, 2015].

[14] Internet Live Stats, 2015-last update, Number of Internet Users (2015) - Internet Live Stats. Available: http://www.internetlivestats.com/internet-users/#byregion [8/24/2015, 2015]

[15] Farooq, A. and Ullah Kakakhel, S.R., 2013. Information Security Awareness: Comparing perceptions and training preferences, Information Assurance (NCIA), 2013 2nd National Conference on 2013, IEEE, pp. 53-57.

[16] Adelola, T., Dawson, R. and Batmaz, F., 2015. Nigerians' Perceptions of Personal Data Protection and Privacy, SQM (Software Quality Management) and INSPIRE (International conference for Process Improvement, Research and Education) Conference, 30th March 2015 2015.

[17] CSEAN, 2015-last update, About CSEAN. Available: http://csean.org.ng/about-csean/ [8/24/2015, 2015].

[18] Oludare, R., 2015-last update, CSEAN kicks off cyber security awareness campaign, expansion | The Guardian Nigeria. Available: http://www.ngrguardiannews.com/2015/07/csean-kicks-off-cyber-security-awareness-campaign-expansion/ [8/24/2015, 2015].

[19] ngCert, 2014-last update, ngCert, About. Available: https://www.cert.gov.ng/about [08/24/2014, 2015].

[20] Information Commissioner's Office, For the public [Homepage of Information Commissioner's Office], [Online]. Available: https://ico.org.uk/for-the-public/ [09/07, 2015].

[21] Central Intelligence Agency, 2015-last update, The world fact book. Available:

https://www.cia.gov/library/publications/resources/the-world-factbook/geos/ni.html [08/25, 2015].

[22] Adelola, T., Dawson, R. and Batmaz, F., 2014. Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches. Regulation, 2, pp. 5.

[23] Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A., 1995. Values, personal information privacy, and regulatory approaches. Communications of the ACM, 38(12), pp. 65-74.

[24] Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. NIST Special publication, 800, pp. 50.

[25] HM Government, 2013-last update, Guiding Principles on Cyber Security. Available: https://www.gov.uk/government/publications/cyber-security-guiding-principles [08/25, 2015].

[26] McCoy, C. and Fowler, R.T., 2004. You are the key to security: establishing a successful security awareness program, Proceedings of the 32nd annual ACM SIGUCCS conference on User services 2004, ACM, pp. 346-349.

[27] McGettrick, A., Cassel, L.N., Dark, M., Hawthorne, E.K. and Impagliazzo, J., 2014. Toward curricular guidelines for cybersecurity, Proceedings of the 45th ACM technical symposium on Computer science education 2014, ACM, pp. 81-82.

[28] Stop Think Connect, 2015 Last update, Keeping the web a safer place for everyone. Available: https://stopthinkconnect.org [8/24/2015, 2015].