Computing, Information Systems, Development Informatics & Allied Research
ISBN 978-2257-44-7(Print) ISSN 2167-1710 (online)
Vol.3 No.1 March 2012

Service Enterprises, Social Engineering and Workforce Productivity – The Case of Zain Nigeria PLC.

Longe, O.B
Fulbright SIR Fellow & Research Scholar
Southern University System
Baton Rouge, LA, USA 70813
longeolumide@fulbrightmail.org

Wada, F.
Research Scholar
Nelson Mandela School of Public Policy
Southern University
Baton Rouge, LA
USA 70813
friwada@yahoo.com

Ukpe, Kufre
Dept. Of Computer Science
University of Ibadan,
Ibadan, Nigeria
ukpekaycee@yahoo.com

ABSTRACT

Apart from contending with the problems of intrusion into enterprise information platforms, organizations are also faced with the consequences of unguided access and usage of social engineering website in the workplace. We examined the circles of network abuse outlined in Network Service Organization's computer use policies using Zain Nigeria Plc as a case study. We designed a questionnaire titled "The Impact of Social engineering websites on organizational productivity" as the research instrument. Using descriptive and inferential statistics, analysis of user responses showed that although some actions are prohibited, employees circumvent the security measures put in place in connivance with some Information Technology department staff. Most employees are also not aware of the far reaching consequences of these seemingly harmless acts on the organization. Recommendations were made based on our findings.
.

Keywords: Enterprises, Social Engineering, Website, Face book, Productivity, Zain

1. INTRODUCTION

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information for gathering or computer system access. In most of the cases the attacker never comes face to face with the victims and the later seldom realize that they have been manipulated. These techniques of information gathering are often carried out through the use of websites (Rusch, 1999). Social engineering websites sometimes referred to as "friend-of a friend" sites are built upon the concept of traditional social networks where one is connected to new or already known people.

The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections. Although the features of social networking sites differ, they all allow us to provide information about oneself and offer some type of communication mechanism (forums, chat rooms, e-mail, and instant messenger) that enables you to connect with other users. On some sites, users can now browse for people through shared connections. Many of these sites have communities or subgroups that may be based on a particular interest. However, these sites generate potential benefits for business organizations, but the area of concern is the security implications posed by the sites.

Social engineering websites rely on connections and communication so that they encourage one to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because the internet provides a sense of anonymity and the absence of physical interaction provides a false sense of security (Longe & Longe, 2005). While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of accessibility and amount of personal information that is available.

As a result, the information could be used to conduct social engineering attack. Social engineering involves luring unsuspected users to take a cyber-bait much the same way a conventional fishing involves luring a fish using the bait. Phishing is a form of social engineering that deceives consumers into disclosing their personal and financial data, such as passwords, ATM pin numbers, credit card numbers and bank account numbers. It is an attempt to elicit a specific response to a social situation the perpetrator has engineered (Tony, 2009). Among other forms of cybercrime, phishing scams are on the increase in Nigeria.

The remaining part of the paper is organized as follows. In the next section we examined some related issues. This is followed by a section highlighting social engineering scenarios in the Nigerian context. We then formulate research questions and elucidate our research methodology. We conclude with recommendations based on the research findings.

2. RELATED ISSUES

Internet social activities have presented marketers with challenges as well as opportunities to reach specific target markets. Facebook emerged on the social network scene over half a decade ago; originally viewed as a networking site limited to college students. In 2006, Facebook was serving as many as 7.5 million registered users and was seventh among the more accessed websites in the U.S. (Collen, 2009; Gaudin, 2002).

Recruiters for businesses and colleges are finding for the social and professional networks are to perform background checks on potential employees. In the past many companies used Google and Yahoo to perform these background checks but recently Facebook, MySpace, Xanga and Friendster are being utilized in this regard (Budden and Budden, 2009). These organizations are looking for "red flags" which might indicate that the potential student or employee might not fit into organizational cultures as expected.

Organizations often gain access to these websites by asking a college student working for the organization to perform the background check. Thus, while some college students think only other students have access to their postings, they are finding that such postings are often times ending up on the desks of potential employers. Granger (2006) pointed out that merely trying to prevent infiltration on a technical level and ignoring the physical-social level leaves organizations wide open to attack. Hollows (2005) explain that while many security systems and technologies have been deployed to prevent intruders from accessing high value systems, an organization simply cannot patch against social engineering.

2.1 The Nigerian Scenario

One area of concern that seems to elude popular debate about social engineering and cyber crime in Nigeria is the potential danger that social engineering poses to business and other organizations in the country. Highly motivated attackers can have much more success by manipulating people (insiders within an organization) rather than trying to hack the various levels of sophisticated security technologies put in place by organizations to secure their operational network. Jason (2009) opined that primal motivators such as fear, greed and sexuality can be used to manipulate employees into releasing information unwittingly thus providing unauthorized access to organizational information systems.

Social engineering therefore constitutes a powerful force that can change the way organizations and the security community perceives insider threats. A casual interrogation of employees in some Nigerian business and financial organizations showed that while on break or when the pressure of work is less, they engage in online chat on social engineering websites using the organization internet facilities (Longe et al, 2010).

Generally, these actions do not fall within the circles of network abuse as outlined in major organizational computer use policies. In some organizations, even though these actions are prohibited, employees circumvent the security measures put in place in connivance with some IT department staff.

Most employees are not aware of the far reaching consequences of these seemingly harmless acts on the organization. Social engineering is the human side of breaking into a corporate network. Cyber criminals cannot be lucky in convincing a firewall to give them access to a bank record, nor can they compel anti-spyware to allow them glean through an organizational database but they could find it easier to persuade a person whose confidence they have gained to allow them admittance.
Access to such secured area of a network or even to disclosure of confidential information can make organizations vulnerable. Nowadays, these criminals explore social engineering websites such as yahoo personals, twitter, zoosk, Facebook and many dating websites as springboards for their attack. By luring employees into a facade of relationships, they use phishing, plant spywares, use anonymous proxy servers and other hacking tools to hack into secured organizational information. For our study, we delimited Zain telecommunications at both Ibadan and Lagos offices as our case studies. We concern ourselves with the use of social engineering websites by the employees of Zain telecommunications as well as its resulting impact on organizational productivity.

2.2. Research Questions

With this increased dependence on online and internet based business transactions and the migration of former paper-based procedures to electronic platforms, research is warranted into the current trends in the use of social engineering websites by employees in organizations, the level of awareness of these risks involved when using these websites as well as measures (if any)

put in place by Nigerian organizations to deal with these problems. The research questions that emanate from the foregoing are as follows:

- What is the level of social engineering websites usage employees in the case study?
- Are employees aware of the threat posed by social engineering websites to their organization?
- What are the mechanisms and policies that are put in place by Zain telecommunication to check the threat of social engineering website?
- What is the level of compliance to the anti- threat mechanism and policies at Zain telecommunication ?
- What are the impacts of social engineering websites' use by Zain employees on organizational productivity?

3. METHODOLOGY

We employed the use of questionnaires as a quantitative research instrument to solicit responses on the level of awareness of risks as well as the level of usage of social engineering websites in the targeted organization. Qualitative interview was carried out among security departments in Zain telecommunications to ascertain the level of preparedness and readiness to deal with social engineering related risks. Descriptive statistical methods of simple frequency counts and percentages were used to analyse the demography and research questions while inferential statistics of T-test was used to analyse the hypothesis.

Hypothesis
To address the research questions, we formulate and analysed the presented hypothesis:

Hypothesis 1
H_0: There is no significant difference in the perceived productivity of employees of Zain Telecommunication as a result of using Social Engineering Websites.

Table 1: T - test on sex of Zain's employees and the use of social engineering websites.

Variables	Mean	Std. Deviation	t.	df	Sig. (2-tailed)	Remark
Sex and the use of social engineering websites	1315	33859	6.152	250	.000	*Sig

Table 1 is a t-test on the sex of Zain's employees and their use of social engineering websites. The table reveals that the result is less than .05 alpha level of significance (t-cal .000 < 0.05 alpha level). Therefore, the null hypothesis is rejected. This is an indication that male and female use of social engineering websites significantly affects employee productivity. Subtly, there is indication that female employees also use social engineering websites than their male counterparts.

Hypothesis 2
H_0: Zain's organizational policies on the use of social engineering websites will not Significantly affect employee's use of social engineering websites at their workplace.

Table 2: T – test policy on website use and employees' compliance

Variables	mean	Std deviation	T	df	Sig (2-tailed)	Remark
Policy on the use of social engineering websites and compliance by employees	- 2072	.56295	-5.830	250	.000	* Sig

Table 2 is a T- test on the use of social engineering websites and the compliance of employees' policy. The table reveals that the t-test is lower than the alpha level of significance .05(t-test cal .000 < .05 alpha level). The hypothesis is rejected. This is an indication that there is a significant difference between the variable tested. Therefore, Zains organizational policy on the usage of social engineering websites will not significantly affect employees' use of the websites at the workplace. The hypothesis is therefore rejected.

4. CONCLUDING REMARKS

Social engineering attacks are one of the hardest threats to defend against because they involve the human element which in itself is quite unpredictable. Nevertheless, there are some measures which can certainly bring the risk associated with social engineering to acceptable levels. While attacks on human judgement are immune to even the best of security defense systems, companies can mitigate the risk of social engineering with an active security culture throughout the organization that keeps on evolving as the threat landscape changes. Findings from this research indicate deviance to organizational policy on social engineering websites usage. This means that the policy does not discourage employee use of the website. The usefulness of the internet resources like social engineering website is not without its shortcoming especially in the corporate world. It has tendencies of affecting workers productivity. This study has established that fact, showing that the use of such websites is detrimental to organizational goals attainment and general wellbeing.

Based on the findings of this study we recommend well documented and accessible security policy, associated standards and guidelines as foundations for acceptable use of web facilities within organizations.

REFERENCES

1. Budden, C & Budden, M. (2009). The social network generation and implications for human resource managers. *Business and Economics Research* 7.1: 10-12
2. Colleen, R (2009):Safeguarding against social engineering. Infosec Writers Library Retrieved May 15, 2010 from http://itmanagement.earthweb.com/secu/article.php/1040881
3. Gaudin, S.(2002). Social engineering: *The Human Side of Hacking*. Retrieved May 2010 from http://itmanagement.earthweb.com/secu/article.php/1040881
4. Granger, S, (2006). Social engineering reloaded. *Security Focus.* Retrieved April 2010 from http://securityfocus.com/print/infocus/1860
5. Jason, H. (2009): Change your company's culture to Combat Social Engineering Attacks .Retrieved May 2010 http://search.techrepublic.com.com/search/Jason%20Hiner%20MCSE.html
6. Longe, O.B & Longe, F.A. (2005). The Nigerian Web Content: Combating the Pornographic Malaise Using Web Filters. Journal of Information Technology Impact. Vol. 5, No. 2 Loyola University, United States of America. www.jiti.net
7. Longe O.B., Mbarika V.W., Jones .C. , Anadi .A., Wada .F. , Longe F.A. , Onifade .O.F.W. & Dada . G. (2010). Can Any Good Thing Come from Nazareth' - An Investigation into the Origins of 419 Spam Mails. Proceedings of the 3nd International Conference of the Int. Centre for IT & Dev. Cameroon, March, 2010.
8. Rusch, J. (1999). *The "Social Engineering" of Internet Fraud.* INET '99 Proceedings. Retrieved April 6, 2010 from http://www.isoc.org/inet99/proceedings/3g/3g_2.htm
9. Hoffman, T.(2007). The Recruit/Retain Shuffle. *Computerworld, 41*(31), 28-32
10. Tony, B. (2009): Gone Phishing http://netsecurity.about.com/od/secureyouremail/a/aa061404.htm

Author's Brief

Dr. Longe Olumide is on Faculty at the Department of Computer Science, University of Ibadan, Nigeria. His research has focused on using social theories and computer security theories to explain causastion and apprehension of cyber crimes. Currently a Fulbright Fellow at ICITD, Southern University's College of Business in Baton Rouge, LA. He can be reached by phone on +18572078409 and through E-mail longeolumide@fulbrightmail.org.

Dr. Friday Wada has a Ph.D in Public policy majoring in Public Finance from Southern University, Baton Rouge, USA. He also holds a Master's degree in Business administration (MBA) from Southern University, Baton Rouge and a Bachelor's Degree and Diploma in Accounting from the Ahmadu Bello University, Zaria, Nigeria. Dr. Friday's research interest is in the area of cyber crime, and his work has been published in journal articles and scholarly presentations made at conferences. He is a recipient of the IGERT/NSF Fellowship award. He can be reached at friwada@yahoo.com.
Phone: +12255880012

Ukpe Kufre holds Bachelor's degree from the University of Calabar, Nigeria, a Master's Degree in Computer Systems from the University of Ibadan, Nigeria and currently pursues a PhD degree at the ICT University, USA. His research findings which has focused on Social and Enterprise informatics has been reported in Journals and presented at conference across the world. He can be reached at ukpekaycee@yahoo.com.
Phone +2348093880292