Journal of Physical Science and Innovation Volume 5, Number 1, 2013.
ISSN 2277-0119

SOCIAL ENGINEERING RELATED ATM FRAUD: A WAY FORWARD

[1]Bulus L.D., [2]Sajoh D.I. and [3]Onyeka N.C.
Department of Computer Science
Federal Polytechnic Mubi, Adamawa State, Nigeria
E-mail: buluslucy08@gmail.com

ABSTRACT
It is well-known that criminals have many ways of illegally accessing ATM card to retrieve money in account of legitimate users. In this paper, brief overviews of the possible fraudulent activities that may be associated with social engineering were provided. Security measures to guide against such problem were also provided. One hundred questionnaires were distributed to respondents; Fig.3 in appendix illustrates the respondents' views in percentage. More so, Table 4 shows the chi-square distribution. Hence, from this study, it can be deduce that people are not making themselves vulnerable to social engineering attacks. Finally, social engineering attacks happened on daily basis it, depends on the way it appears to users of the ATM card.

Keywords: Social Engineering, Fraud, ATM, Security and Phishing

INTRODUCTION

Throughout history, criminals have often engaged in unauthorized acquisition and use of another person's identity to obtain some advantage they are not entitled to receive[13]. [1]States that Automated Teller machine (ATM) is basically a cash dispenser, it has a unique service of 24/7 facility, "stand alone" or "wall mounted". Fraudsters deceive and manipulate people, exploring human weaknesses through the use of ATM related fraud to obtain personal benefit. They use social engineering techniques as part of Information Technology (IT) fraud. The customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip, which contains a unique card number and some security information such as an expiration date. Authentication is provided by the customer entering a personal identification number (PIN). Using an ATM, customers can access their bank accounts in order to make cash withdrawals or check their account balances as well as pay their bills[9].

Fraud is dishonesty calculated for advantage. A person who is dishonest may be called a fraudster. It is an independent criminal offense, though appears in different contexts as the means used to gain a legal advantage and it involves more planning[3].This fraud has the tendency of discouraging people from using their ATM card. Therefore there is need to prevent fraud as much as possible. [5]Explained that reducing fraud to the minimal will help both the Banks and the customers to understand each other in terms of business. This will also build customer confidence and increase the Bank's reputation in comparison to its competitors. [11]Studied the form in which Social Engineering can appear. He said, if a person pose as responsible and makes another person believes that he/she could be trusted with ATM card and PIN code. Typical Example is posing as a bank officer. Customer's card may get stuck in an ATM machine by some installed device and the customer needed help from the bank officers present; thereby rings up the emergency phone number pasted on the ATM point. The fraudler on the other side identifies himself as the bank employee and can offer help. For that he needs the customer PIN and the customer gave him the PIN. The card is retrieved later by the fraudler.

Social engineering websites sometimes referred to as "friend-of a friend" sites are also built upon the concept of traditional social networks where one is connected to new or already known people. 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[12]. [10]Observed that Social engineering can appear in different forms, depending upon where someone sits. Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to valuable information. As pointed by[8] Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Social engineers take advantage of people's natural understanding to choose passwords that are meaningful to them but can be easily guessed especially with ATM card PIN.

A study by[7] clarified that Social engineers use influence and persuasion to deceive people for the purpose of obtaining information to perform some action. He further stated that a social engineer commonly uses the telephone or Internet to trick people into revealing sensitive information. Basically two common types of attacks exist, these are:

i. **Human-based:** Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password. Human-based social engineering techniques can be broadly categorized as follows:

   a. ***Posing as an important user:*** In this type of attack, the hacker pretends to be an important user such as an executive who needs immediate assistance to gain access to a computer system or files. The hacker uses intimidation so that a lower-level employee such as a help-desk worker will assist them in gaining access to the system. Most low-level employees won't question someone who appears to be in a position of authority.

   b. ***Using a third person:*** Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or can't be contacted for verification.

   c. ***Shoulder surfing:*** Shoulder surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system. A hacker can watch a valid user log in and then use that password to gain access to the system.

ii. **Computer-based:** Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an e-mail and asking them to re-enter a password in a web page to confirm, it employs a computer in the attack. Computer-based social engineering attacks can include the following:
   a. E-mail attachments
   b. Fake websites
   c. Popup windows

Another form of social engineering is phishing, as studied by[12] "Phishing" is a criminal mechanism employing social engineering to steal customer's personal identity data and financial account details. It is a form of social engineering that deceives customers' into disclosing their personal and financial data, such as passwords, ATM PIN, credit card numbers and bank account numbers. Among other forms of crime, phishing scams are on the increase in Nigeria. In [11], phishing technique is said to be mostly used by hackers to obtain confidential details of bank password via email and sometimes they collect ATM card PINs. The customer believes in the e-mail looking exactly like his banker's asking for personal details, password, PIN code etc., and blindly complies with the request and through that they invade into his account, see fig. 1 below.

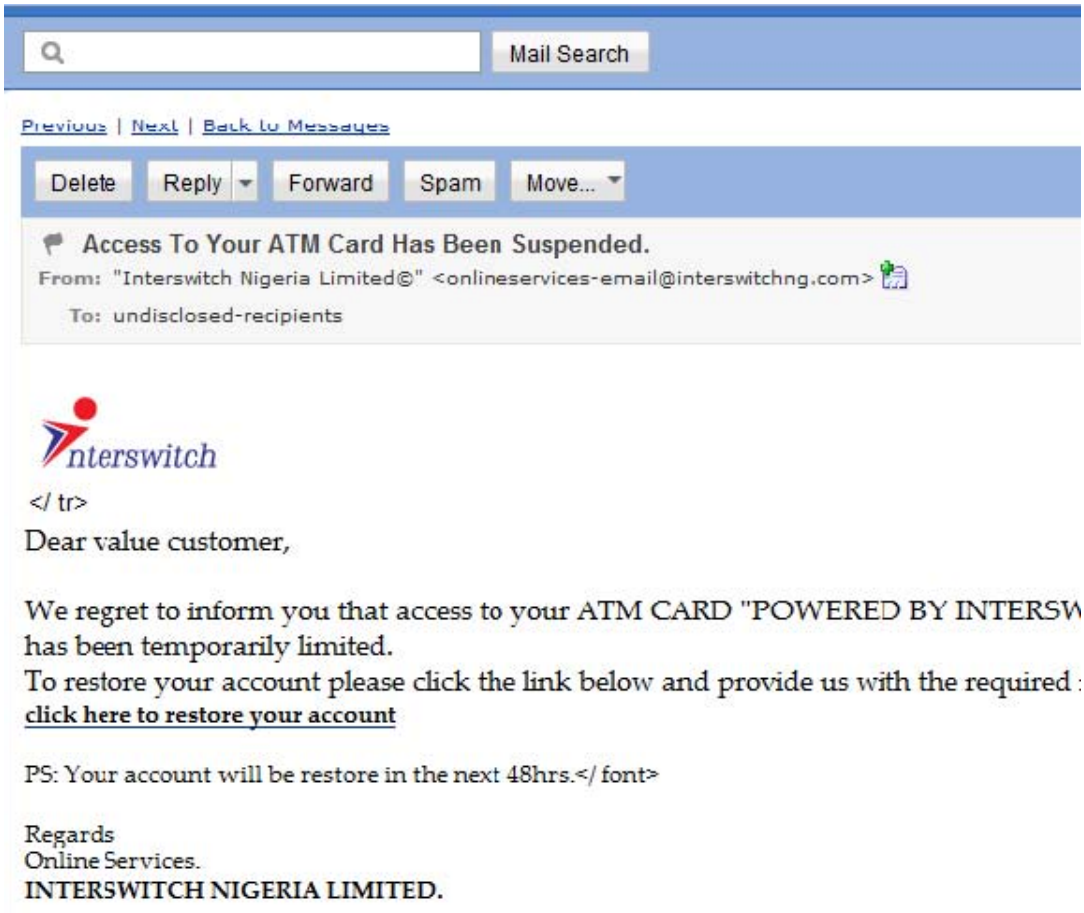

Fig. 1: 419 Scam for Phishing[2]

Social engineering is the art of manipulating people, for instance criminals cannot just be lucky in convincing a bank to give them access to individual account detail, nor ATM card details but they could find it easier to persuade a person who they met at their own end and are loose in disclosing confidential information. This paper therefore, evaluate peoples' vulnerability to social engineering attacks and proffer solution now and in the near future, such that much will not be lose to social engineering attacks.

RESEARCH QUESTION
Are people making themselves vulnerable to social engineering attacks?

HYPOTHESIS
H_0: People are making themselves vulnerable to social engineering attack.
H_1: People are not making themselves vulnerable to social engineering attack.

MATERIALS AND METHOD
Questionnaire was used to find out the respondents view if actual they are making themselves vulnerable to social engineering attacks. One hundred Questionnaires were issued out to respondents in Federal Polytechnic Mubi, Adamawa State-Nigeria.

INSTRUMENT FOR DATA COLLECTION
The research instrument is the questionnaire, titled "Social Engineering Related ATM Fraud: A Way Forward" was administered to respondents.

RESULTS AND DISCUSSION
One hundred questionnaires were issued out, ninety nine (99) were returned filled; respondents' sex and age groups were specified. From Table 1, the study revealed that 68% of the population are men, while 32% are female. The study further examined age groups, 15-24, 25-34, 35-44, and 45 & above representing 12%, 46%, 27% and 14% respectively in Table 2. Based on this study, youth engage much in the use of ATM card having 46% of the responses.

From Fig.3, 94% of the respondents have ATM and 6% do not have ATM cards. Question two further give 92% of those people that keep ATM in their custody, whereas 8% do not keep it in their custody. 98% of the ATM card holders use it to withdraw money, whereas 2% don't use it for withdrawal of money from the bank. When withdrawing with ATM card, 38% look for assistance from second party, while 62% do not required help in withdrawing. On equal note, 46% send second party to help them withdraw money from the bank, whereas 54% go themselves.

In terms of disclosure of card details to other party, 46% agreed while 54% disagreed to that. We further established the fact that 48% of the respondents discussed ATM card issue with second party while 52% did not. About 21% of the respondents have posted their card details online and also sent using their mobile phone whereas 79% have not. Question ten further states that 84% of these respondents agreed that they are not compromised in using ATM card to withdraw money while 16% disagreed.

Table 3 shows common related exposure of the ATM card responses while Table 4 shows the chi-square distribution. From Table 4, we reject the null hypothesis and accept the alternative hypothesis which, state that users of ATM are not making themselves vulnerable to social engineering attacks but depends on the way it appear to the users of ATM card.

WAY FORWARD
Social engineering attacks are on the increased, but we can manage the situation if and only if every single person would take the responsibility of his/her actions. Among these are:

i. ***Avoid Over Helpful Hands:*** Another way criminal get PIN numbers is by hanging out near and offering help when the unit fails to "work." A helpful bystander will offer to help and ask for the person's PIN. Of course, once they have it, the card is as good as theirs.

ii. ***Cover Your Pin While Withdrawing***: Another way skimmers get PIN info is by installing small, hidden cameras somewhere inside the machine. They can be in the wall, or even hiding inside marketing materials, like pamphlets which appear to be innocently sitting off to the side. [6]Suggested covering PIN with hand, even when one is alone. This may prevent a camera from detecting it see fig.2 below.

Fig.2: Hand Covering During ATM Card Usage[11]

iii. ***Monitor Accounts Regularly***: Regular monitoring will keep one on top of any suspicious activity that may occur as the result of a compromised account. Reporting fraudulent activity as quickly as possible gives one the best possible chance to recover losses.

iv. Always keep confidential data safe.

v. Know how to change password, how often to change the passwords, who gets access to your information, and destruction of paper documents regarding confidential information.

vi. Identifying which information is sensitive and evaluating its exposure to security systems.

CONCLUSION

According to[12], Social engineering attacks are one of the difficult aspects that should not be treated carelessly. It constitutes a powerful force that can change the way an innocent man think and the security solution to it. Social engineering relies on the fact that people are not aware of the value of information they possess in term of security and are careless about protecting these information. We need an urgent call to social engineering consciousness and the way we handle the ATM card.

Furthermore, this paper is an attempt to equip the users of ATM on the need to know related social engineering fraud in the ATM system. Fraud is preventable; it can be closely monitored in order to reduce the consequences and frequencies of occurrence in the future. Always proceed with caution, guard your personal information both online and offline; never

disclosed your ATM card PIN to anyone, above all to strangers who e-mail you and claim to be from your bank.

ACKNOWLEDGEMENT
All respondents of the questionnaires are highly acknowledged especially the staff of Computer Science Department, Federal Polytechnic, Mubi-Nigeria.

REFERENCES

1. I.D. Adewuyi (2011): Electronic Banking in Nigeria: Challenges of the Regulatory Authorities and the way Forward, *International Journal of Economic Development Research and Investment*, Vol. 2 No. 1; April 2011 149-156,

2. N.A. Azeez, and I. Barry (2010): Cyber Security: Challenges and the Way Forward, GESJ: Computer Science and Telecommunications 2010 No.6(29) , ISSN 1512-1232, Accessed May 2nd 2013 from http%3A%2F%2Fgesj.internet-academy.org.ge

3. *N. H. Gerald, and T. H. Kathleen (2005) Legal Dictionary, Access May 2 2013 from* http://legal-dictionary.thefreedictionary.com/fraud

4. C.O. Ikem, (2003): Research Manual, Guide for Research in Applied Science, Education Technology, Medicine, Engineering and Business Studies, Paraclete Publishers, Yola, Nigeria

5. K. Janet, (2011): Fraud Risk Assessment Plan for Barclays Bank of Kenya, Bachelor's Thesis, December 2011, Tampere University of Applied Sciences, Access May 13 2013 from http://publications.theseus.fi/bitstream/handle/10024/38379/Kimani_Janet.pdf?sequence=1

6. G. Joan (2010): ATM Skimming: How to Recognize Card Fraud, Access May 7 2013 from http://www.csoonline.com/article/555863/atm-skimming-how-to-recognize-card-fraud

7. G. Kimberly, (2007): Official Certified Ethical Hacker Review Guide, Wiley Publishing, Inc., Canada ISBN-13: 978-0-7821-4437-6. Pg. 28-37

8. R. Margaret, (2006): Security Technology target, Accessed May 6 2013 from http://www.searchsecurity.techtarget.com/definition/social-engineering

9. SADAD (2012): Automated Teller Machines, Kingdom of Saudi Arabia - Riyadh, 2013163, Access May 7 2013 from http://www.sadad.com/English/Pages/default.aspx

10. G. Sarah, (.2010): Social Engineering Fundamentals, Part I: Hacker Tactics, Access May 5 2013 from http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker tactics

11. T.S. Subramanian, (2012): ATM Vulnerabilities, Frauds and Crimes, pg. 107-111, Access May 1 2013 from http://220.227.161.86/28021cajournal_oct2012-22.pdf

12. K. Ukpe, A. Salami, G.O. Odulaja, Z.A. Mahmood, R.Omotoso and E.S Mughele (2011): Social Engineering and Workplace Productivity-Balancing the Odds, *African Journal Computer & Information Communication Technology* , Vol 4. No. 1. June 2011, pp.51-54

13. United States of America (2010): A Report to the Attorney General of the United States and the Minister of Public Safety of Canada (November, 2010); Identity-Related Crime: A Threat Assessment, Access May 10, 2013 from http://www.justice.gov/criminal/fraud/documents/reports/2010/11-01-10mass-market-fraud.pdf

APPENDIX

Table 1: Respondents Sex

Sex	Frequency	Percentage (%)
Male	67	68
Female	32	32
Total	**99**	**100**

Source: Field Survey, 2013

Age group	Frequency	Percentage (%)
15-24	12	12.1212
25-34	46	46.4646
35-44	27	27.2727
45 & above	14	14.1414
Total	**99**	**100**

Source: Field Survey, 2013

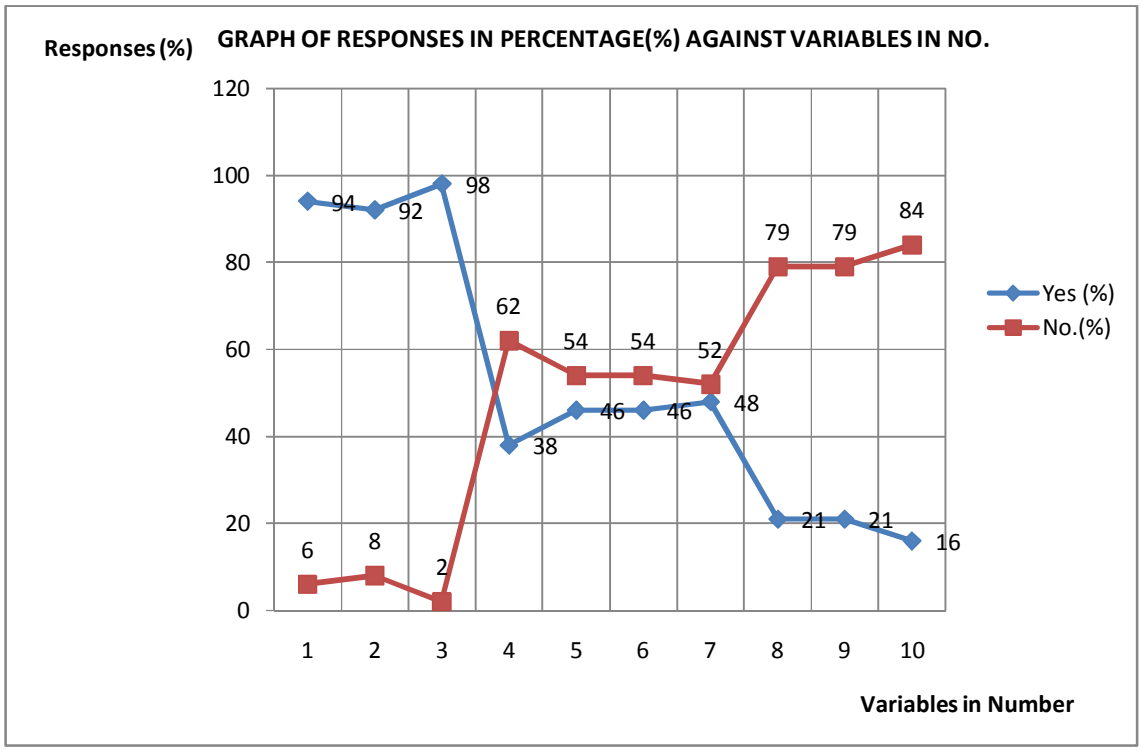

Fig.3 Respondents Responses (*Source*: Field Survey, 2013)

Table 3: Common Related Exposure of the ATM Card

No./Responses	Yes	No	Total
1	91	2	93
2	35	56	91
3	42	49	91
4	42	49	91
5	44	47	91
6	19	72	91
7	19	72	91
Total	**292**	**347**	**639**

Source: Field Survey, 2013

$$C_{ij} = \frac{(RxC)}{G}$$

Table 4:Chi-square Computational Table

O	E	O-E	$(O-E)^2$	$(O-E)^2/E$
91	42.5	48.5	2352.25	55.34706
35	41.58	-6.58	43.2964	1.041279
42	41.58	0.42	0.1764	0.004242
42	41.58	0.42	0.1764	0.004242
44	41.58	2.42	5.8564	0.140847
19	41.58	-22.58	509.8564	12.26206
19	41.58	-22.58	509.8564	12.26206
2	50.5	-48.5	2352.25	46.57921
56	49.42	6.58	43.2964	0.876091
49	49.42	-0.42	0.1764	0.003569
49	49.42	-0.42	0.1764	0.003569
47	49.42	-2.42	5.8564	0.118503
72	49.42	22.58	509.8564	10.3168
72	49.42	22.58	509.8564	10.3168
				149.2763

Source: Field Survey, 2013

X^2 = chi- square value, O = observed value, E = expected value

$X^2_{tab} = (R-1)(C-1)$, df = (7-1)(2-1)= 6, 5% = 12.592 ;$X^2_{cal} = \sum_{i=1}^{n} \frac{(O_{ij}-E_{ij})^2}{E_{ij}}$, $X^2_{cal} =$ 149.28

Decision Rule: x^2_{cal} 149.28 > $x^2_{tabl.}$ Therefore, we reject the null hypothesis and accept the alternative hypothesis. Hence conclude that people are not making themselves vulnerable to social engineering attacks but depends on the way social engineering appear to the users of ATM card.

Reference to this paper should be made as follows: Bulus L.D., Sajoh D.I. and Onyeka N.C. (2013), Social Engineering Related ATM Fraud: A Way Forward, *J. of Physical Science and Innovation, Vol.5, No.1, Pp. 106-115*.

Biographical Note: Bulus, Lucy Dalhatu obtained her B.Sc. in 2007 from Adamawa State University, Nigeria and at present a Master student in Computer Science at Adamawa State University.

Biographical Note: Sajoh, Dahiru Ibrahim He got his M.Sc. in Software Engineering from De Montfort University, Leicester in 2012, obtained B.Tech. in Computer Science from Federal University of Technology Yola, Nigeria, in 2008. His research interest includes Software Engineering, Pervasive System and Artificial Intelligence.

Biographical Note: Onyeka, Ndidi Camilia she is a Lecturer with the Computer Science Department, Federal Polytechnic Mubi, Nigeria. She holds M.Sc. in Computer Science from University of Ibadan, Nigeria. Her research interests include Information Security, Social Networks, Software Engineering and Pervasive Systems.