The African Journal of Information Systems

Volume 3 | Issue 1 Article 2

4-2011

On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers

Olumide Longe
University of Ibadan, longeolumide@ieee.org

Adenike Osofisan
University of Ibadan, nikeosofisan@gmail.com

On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers

Research Paper

Volume 3, Issue 1, April 2011, ISSN 1936-0282

Olumide Longe

Department of Computer Science,
University of Ibadan
Ibadan, Nigeria
longeolumide@ieee.org

Adenike Osofisan

Department of Computer Science,
University of Ibadan
Ibadan, Nigeria
nikeosofisan@gmail.com

(*Received December 2010, accepted March 2011*)

Abstract

One issue that is concerning to the web security community is the correct identification of the origins of advance fee fraud mails. This has serious implications for directing concerted efforts towards mitigating the malaise in the right direction. Although previous research (Cuckier et al, 2007, Gbenga, 2007; Igwe, 2007; Progame, 2007) opined that these mails originate mainly from Nigeria and other West African Countries, research is warranted using available tracking tools to validate previously held notions about the issue of advance fee e-fraud mails. We harvested in real-time aggregated advance fraud e-mails over a two year period using the sinkhole aggregation methodology as proposed by Abhinav et al (2008), Using freeware e-mail and internet protocol address tracers, we obtained results that deviates from the generally held believes about the origins of advance fee fraud e-mails. Our findings have implications for research on spam filtering and by extension web security.

Keywords : *Spam, Advance fee fraud Mails, Nigeria, Africa, E-Mail Tracers, Origin*

1. INTRODUCTION

It is generally believed that most fraudulent mails in cyberspace and phishing attacks originate from or are traceable to Nigeria and some other countries in the West African coast. In addition to these are the

emergence and prevalence of phishing scams using social engineering tactics to obtain online access codes such as credit card numbers, bank account details, social security number, ATM pin numbers and other personal information. A new dimension in the problem domain is the evolution of dating sites purportedly seeking to connect eligible bachelors to spinsters as well as sites for obnoxious activities such as sites dedicated to married people looking for fun and sexual escapades outside the borders of their marriage. These genre of web-based fraudulent activities coupled with the ubiquitous nature of the internet continue to make the issue of ethics and safety topical and worrisome among internet users all over the world. Although the use of rich narrative in these mails appeals to strong emotions and invokes archetypal myths of windfall fortunes that get victims to fall for these scams (Cuckier et al, 2007) scientific research is warranted to validate these assumptions in the light of new and emerging technologies such as e-mail address and IP address tracers that allow users track the origin of fraudulent e-mails.

2. RELATED WORKS

Technically, efforts at controlling and mitigating cyber crime have concentrated on the development of filters and anti-phishing software such as E-Mail address Encryptors, the use of an outbound filtering systems as a measure to stem the volumes of spam mail at their origin and the use of support vector machines (SVMs) and Bayesian systems to train spam filters (Longe and Chiemeke, 2006; Peter, 2006; Tony, 2009; Longe et al, 2008). In his thesis, Tenfa (2006) posited that advance fee fraud is a global problem that requires a global solution. Holt and Graves (2007) carried out a qualitative analysis of advance fee fraud email Schemes and opined that the problem is escalating in size and dimension. Olowu (2009) called for an Inclusive framework for Africa after examining the cyber crime problem in the light of national boundaries, the sovereignty of the laws of nations and boundaries of domestic legal responses. Oriola (2005) evaluated Nigeria's Regulatory Response to advance fee fraud and found them inadequate. Reich (2004) discussed advance fee schemes across borders and traced the origins to Nigeria and some West African Countries. Russell (2001) proposed an agenda for the reformation of laws and policies to deal with advance fee fraud. Profgame (2007) present poverty as a driving force for cyber crime in Nigeria. Ampratwum (2009) showed the link between crime rate and development and posited that there is a need for transnational collaborative efforts in combating these crimes. Ribadu (2007) present a nexus view of the cyber crime problem and called for collaboration between law enforcement agencies across the world to join hands in militating against the cyber crime problem. Gbenga (2007) address the causes and effects of the menace of Cyber Crime in Nigeria and proposed youth empowerment in terms of employment and financial aid as tenable solutions.

3. EMERGING TRENDS

Information provided by the United States Internet Crime Complaint Centre (USIC3, 2009) between 2006 and 2008 (Tables 2 and 3) brings the advance fee fraud mail issue to the fore as Nigeria maintained a high position among the first ten nations as the origin of Spam mails. Confidence fraud, computer fraud, check fraud, and the 419 mail round out the top seven categories of complaints referred to law enforcement during the year. Of those complaints reporting a dollar loss, the highest median losses were found among check fraud ($3,000), confidence fraud ($2,000), Nigerian letter fraud (West African, 419, Advance Fee) ($1,650). Diplomatic missions around the world warn visitors to various West African countries such as Nigeria, Côte d'Ivoire, Togo, Senegal, Ghana, Burkina Faso and Benin Republic of susceptibility to 419 scams. Countries outside of West Africa with 419 warnings are South Africa, Spain, and The Netherlands.

Table 1: Amount Lost by Selected Fraud Type for Reported Monetary Loss

Complaint Type	**% of Reported Total Dollar Loss**	**Average (median) $ Loss per Complaint**
Nigerian Letter Fraud	1.7%	$5,100.00
Check Fraud	11.1%	$3,744.00
Investment Fraud	4.0%	$2,694.99
Confidence Fraud	4.5%	$2400.00
Auction Fraud	33.0%	$602.50
Non-delivery	28.1%	$585.00
Credit/debit Card Fraud	3.6%	$427.50

Source: Internet Crime Complaint Centre Report (2006-2008) - http://www.ic3.gov/media/annualreports.aspx

The effect of fraudulent spamming activities can be measured by the pressure volumes of spam messages places on internet bandwidth, thus slowing it down. This is not helpful in an age when subscribers are clamouring for faster connections. It also increases the dial-up costs by extending the time a person spends reviewing e-mail. When Spammers use false e-mail addresses and users attempt to respond to them, the e-mail bounces around in cyberspace loops creating huge administrative loads for Internet infrastructures. Other hidden costs involve the claims made on two precious human resources: time and energy. Computer users can spend hours attempting to identify the original sender of an e-mail. Research has shown that out of the estimated 30 million e-mail messages each day, about 30% on average are unsolicited commercial and fraudulent e-mails (Deborah, 2005). Chiemeke & Longe (2008) projected that spamming will cost 1.4 percent of employee productivity, or N131,100 per year per employee in Nigeria, the equivalence of $874 in the US. Filtering Spam is therefore an extremely urgent problem. With the escalation in the volume of spam mails on the webscape, organizations are also being subject to mounting pressure to deal with issues regarding employee productivity, morale, sexual harassment and congestion of the e-mail infrastructure.

Table 2: Top Ten Countries - Perpetrator of Cybercrime

Year 2006		**Year 2007**		**Year 2008**	
United States	60.9%	United States	63.2%	United States	66.1%
United Kingdom	15.9%	United Kingdom	15.3%	United Kingdom	10.5%
Nigeria	5.9%	Nigeria	5.7%	Nigeria	7.5%
Canada	5.6%	Canada	5.6%	Canada	3.1%
Romania	1.6%	Romania	1.5%	China	1.6%
Italy	1.2%	Italy	1.3%	South Africa	0.7%
Netherlands	1.2%	Spain	0.9%	Ghana	0.6%
Russia	1.1%	South Africa	0.9%	Spain	0.6%
Germany	0.7%	Russia	0.8%	Italy	0.5%
South Africa	0.6%	Ghana	0.7%	Romania	0.5%

Source: Internet Crime Complaint Centre Report (2006-2008) - http://www.ic3.gov/media/annualreports.aspx

4. RESULTS

In Table 2 the ICC report for the period 2006-2008 reflects that the United States tops the list of nations that perpetuates cyber crime (62% - 66.1% in three years). This is followed by the United Kingdom where cybercrime activities by percentage dropped from 15.9% to 10.5% between 2006 and 2008. Nigeria is third on the list with a marginal increase of 1.6% between 2006 and 2008. Two other African countries ; Ghana and South Africa are also listed in the midst of other European and Asian nations. What the above Table did not reflect is that typology of these cybercrimes. Even though the United States is consistently ahead of other nations in terms of cyber criminal activities as reflected in the table, the diversity of cyber criminal activities responsible for the figure include advertisement spam, cyber pornography, product marketing bulk mails and so on. However, a focus on cyber fraud in Table 1 show that monetary loss due to advance fee fraud tops the list of reported dollar loss to cyber criminal activities. This unfortunate scenario begs the questions – are these loses traceable to mails that emanate from Nigeria and other West African Countries?

4.1 IMPLICATIONS

Against the backdrop of Advance fee fraud mails, it is feasible to ask the question: 'Why do they continue to exist and where do they come from?' The answer to this is simply that no matter how strange a concept it may seem, Spammers get results. A small percentage of email users actually do fall for the bogus financial proposals in Advance Fee Fraud or 419 mails – named after this section of the Nigerian Financial Crime Code. While the public perception of Spam is largely negative, Spammers would not be operating if it were not a viable source of income. They only needs to receive one hundred responses out of ten million Spam messages (0.001% acceptance) to turn a profit. Within the last decade, the use of the Internet in Africa has grown so rapidly with the explosion of Internet Service Providers (ISPs), Internet cyber cafés and access points. This has had several positive impacts on the social, economic and educational sectors in these nations. Unfortunately, the image of nations such as Nigeria, Ghana and Cameroon has also suffered as a result of the nefarious activities of some users, who instead of utilizing the Internet for constructive purposes, turn it into a cheap channel for the perpetration of criminal activities, especially the 'Advanced Fee Fraud (AFF). Nigeria in particular has therefore gained recognition as a source of fraudulent Spam mails characterized by bogus business proposals and fraudulent joint ventures.

If these mails do not entirely emanate from the suspected nations , then spammers have scored another point by allowing efforts to be directed and focused solely on a few nations in Africa that only contribute a small percentage to the advance fee fraud problem. Since most of these nations don't even have reliable databases for apprehended cyber criminals, these criminals can simply change location, move to other nations even in the western world and perpetuate their heinous crimes. The increase in the volume of cyber criminal activities noticed in the United States, Canada and part of Europe may be a consequence of these scenario. Are spammers migrating to the western world from resource-poor regions of the worls; sub-saharan Africa in particular - The implications for cyber security and information systems research is that measures must be adopted that correctly identify causation, locate criminals in order to direct preventive efforts in the right direction and provide appropriate treatments. This is what we set out to do in this research.

5. EXPERIMENTS

We adopted but modified the sinkhole methodology in real-time as proposed by Abhinav et al (2008). Our e-mail accounts were activated and used from locations outside Nigeria, specifically in the United States of America and United Kingdom and Canada to ascertain the source of these mails. Subscription to all forms of online promotion and marketing were avoided in order to avoid other forms of spam. We received over 36,000 fraud spam mails over a two year period.

Tracking Sources of 419 E-Mails

We selected 400 electronic mails randomly from our corpus of spam mails harvested over time. To find the actual location from which the e-mail originates we pick the "Received From" IP that is at the bottom of the list on the header view. We run the e-mails through specific open-source e-mail and IP address tracers such as IPSLocator, E-Mail Trace, and IPGeolocator. We obtained the result show in the table and figures below.

Table 3: Advance Fee Fraud E-mail Distribution by Continents

Country	Percentage of 400 Mails
AMERICA AND CANADA	**28.5**
EUROPE	**23.2**
AFRICA	**20.4**
SOUTH AMERICA	**15.2**
ASIA	**9.5**
AUSTRALIA	**4.2**

For a letter purportedly originating from Kuala Lumpur claiming that there is a lottery Jackpot that has been won, the trace showed that the letter emanated from Brazil South America.

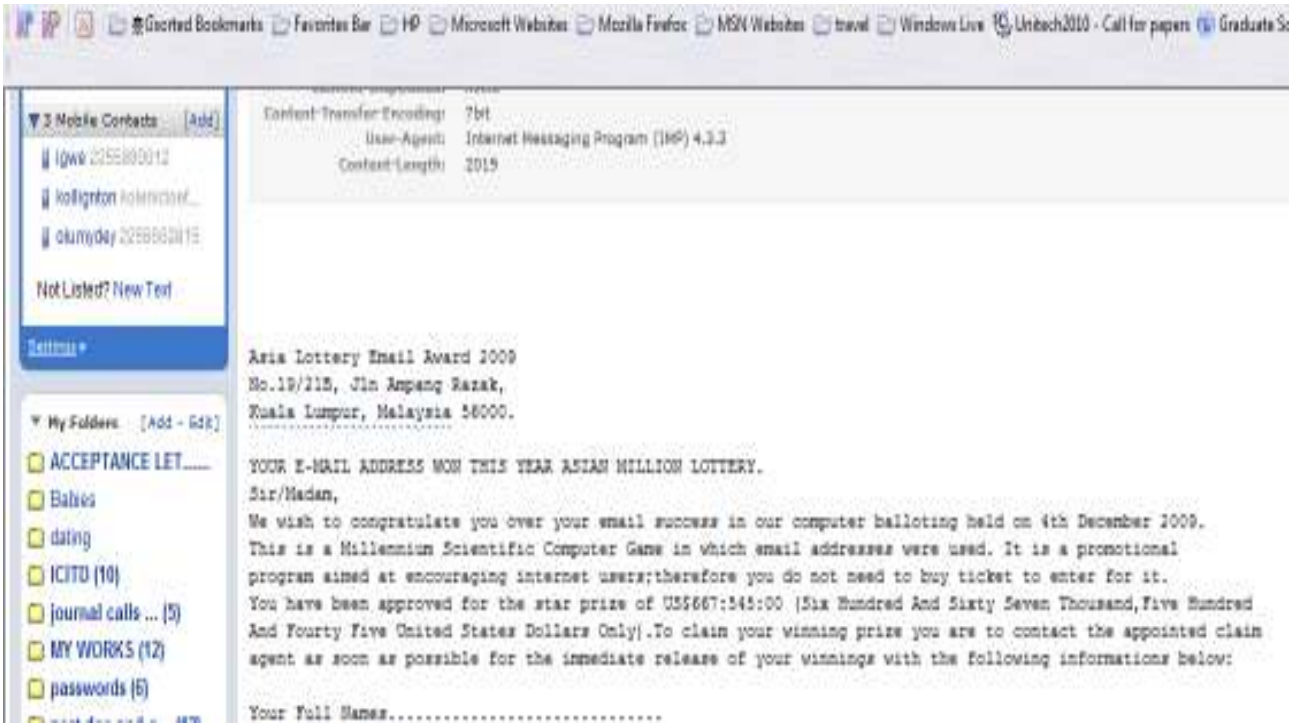

Fig. 1: Screenshot of e-mail purportedly from Kuala Lumpur

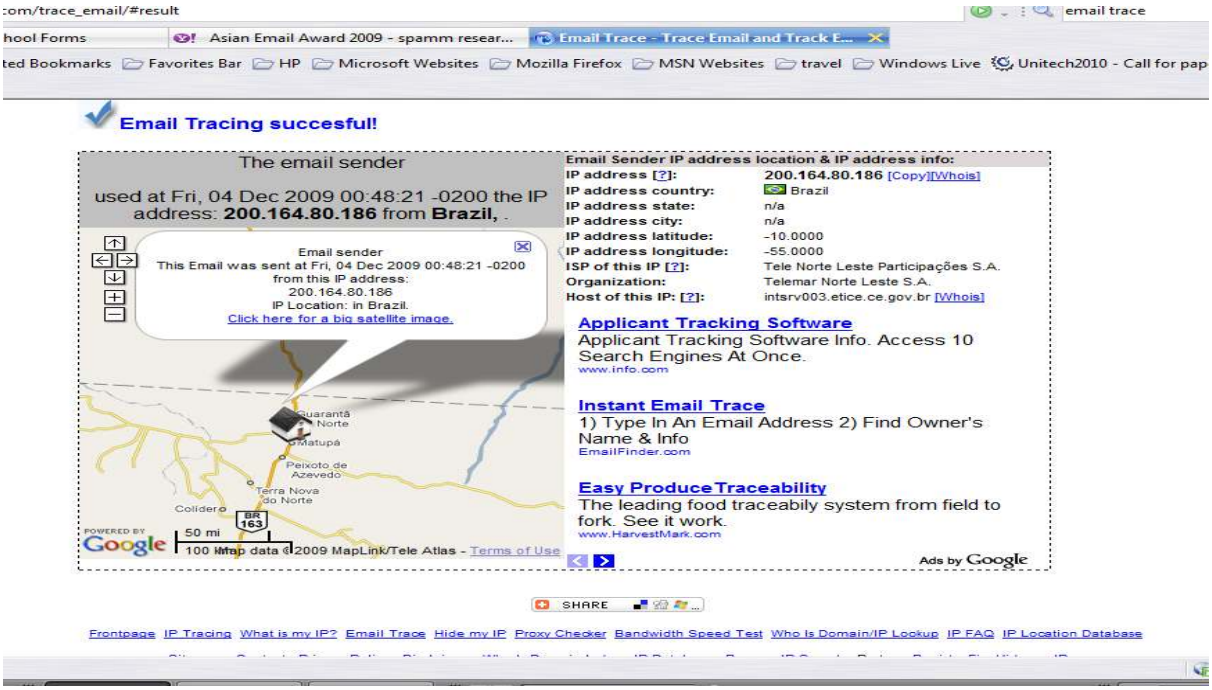

Fig. 2: E-Mail trace result for the email showing it originates from Brazil

The analysis of an e-mail claiming to originate from Interswitch Nigeria Limited with the message ***"an account has been suspended and personal details should be provided for reactivation"*** provided the following analysis

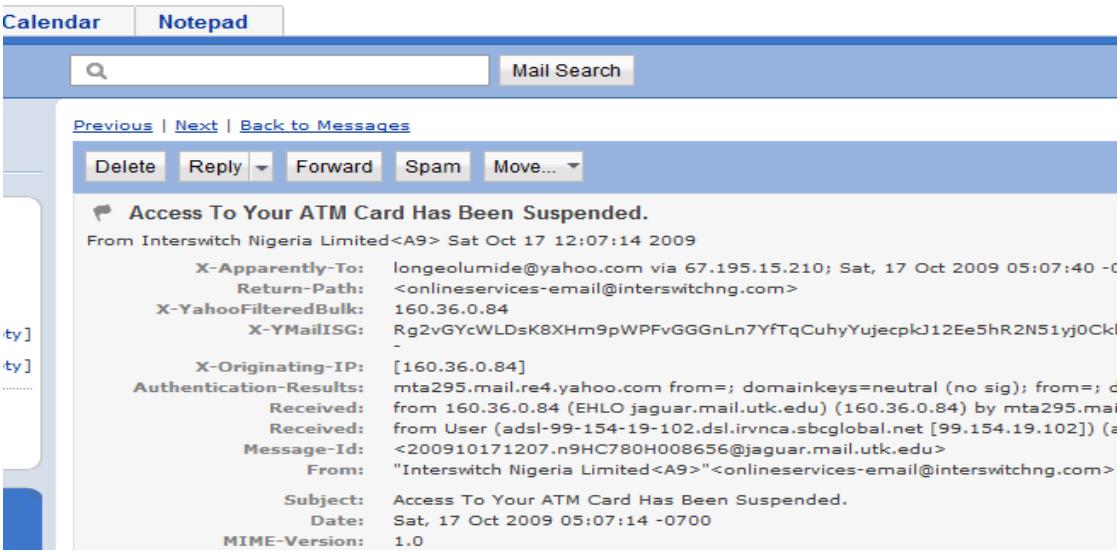

Fig. 3: Letter Purportedly from Interswitch Nigeria Limited

IP Address	Country (Short)	Country (Full)	Flag	Region	City	ISP	Map
160.36.0.84	US	UNITED STATES		TENNESSEE	KNOXVILLE	UNIVERSITY OF TENNESSEE	MAP IT!
160.36.0.84	US	UNITED STATES		TENNESSEE	KNOXVILLE	UNIVERSITY OF TENNESSEE	MAP IT!
160.36.0.84	US	UNITED STATES		TENNESSEE	KNOXVILLE	UNIVERSITY OF TENNESSEE	MAP IT!

Fig. 4: Result from IP2Location on the validity of the IP address

Table 4: Different forms of e-mail harvested from our experimental e-mail accounts.

Type	Spamming Technique Employed	Total No of Mails (%)
Bayesian Poisoning	E-mail with links to other websites with an e-mail body filled with meaningless sentences to confuse the	35

	Bayesian filters using tokens manipulations i.e AgeiNg numbe3rs etc.	
Dating Spam	E-mail in response to dating site activities asking for funds transfer, pictures or photographs of the recipient etc.	22%
Spoofing/phishing	Fictitious sender addresses usually direct users to respond to an entirely different address(es) from the sender address. Usually, the two addresses looks similar. i.e akinadekolapo444@yahoo.com kolapoakinade444@yahoo.com	17%
Academic Spam	For conference Invitation – variations in the from e-mail address and the required e-mail address for communication	13%
Attachment Only E-mail	These e-mails contain just an attachment or two with no contents at all.	9%
Individually targeted e-mail	Electronic mail targeted at individuals with concrete correct information purportedly asking for funds transfers to a friend(s) in trouble or stranded somewhere far abroad	4%

6. DISCUSSIONS

From the Table above, one very disturbing trend in the spam war is the emergence of individually targeted e-mails and academic conference(invitation) spam e-mails. Quite a number of individuals have fallen victims to this genre of spam. The fraudsters use key-loggers and acess to privileged information on individual such as travel itineraries to target unsuspecting victims. Findings from our experiment also showed that advance fee fraud e-mails do not only emanate from Nigeria and some West African nations, a bulk of them are beginning to originate from the western world (America and Europe) the middle east and part of Asia. This is concerning as it reflects the fact that a focus on Africa or West Africa in particular as the major source of fraudulent mailing and cyber activities as is the norm is misleading. This fact is exacerbated by the emergence and prevalence in the middle east of cyber criminal activities, portending grave dangers for other part of the world that are already apprehensive on the fear of cyber terrorism. It remains to be investigated if the increase noticeable in the volume of fraudulent spamming activities emanating from other part of the world is correlated with the number or volumes of Africans, Asians and other immigrants' moving into the western nations.

As the internet expands, opportunities for unethical use will continue to increase if nothing pragmatic is done in terms of policies, technology and law to protect users against online criminals. This is reflected in the routine activity theory which posited that crime can be motivated by opportunities provided in routine activities. Incidentally, the use of the web falls perfectly into the domain of routine activities hobeit on a global scale. (Cohen et al, 1979; Felson & Cohen, 1993). Correlating poverty with cyber crime as a major factor that points to Africa and some resource-poor environment as the source of advance fee fraud mail may not capture the

entire picture and could be misleading. Future research will explore the contributions of other subtle but extraneous factors such as the economic meltdown and immigration policies on the increase in fraudulent cyber activities now noticeable in the western world.

7. CONCLUDING REMARKS

Citing the example of the increase in the wave of crime after World War II despite the booming economy and expansion of the Welfare states Cohen & Felson (1993) argued in support of the routine activity theory that the prosperity of contemporary society offers so much opportunities of crime since there is much more to steal. The premise of our argument is that most cyber crimes go unreported to law enforcement agencies and may not be necessarily be influenced by social factors such as poverty, inequality and unemployment (Longe, 2008b). Research and policy will have to focus on identification, causation and treatment to be able to combat the cyber crime menace.

REFERENCES

Abhinav Pathak , Y. Charlie Hu , Z. Morley Mao, Peeking into spammer behavior from a unique vantage point, Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, p.1-9, April 15-15, 2008, San Francisco, California

Ampratwum, E. (2007) Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA). Journal of Financial Crime, Vol. 16 No. 1,pp. 67-79

Clarke, R. V. and M. Felson (Eds.) (1993). Routine Activity and Rational Choice. Advances in Criminological Theory, Vol 5. New Brunswick, NJ: Transaction Books

Cukier Wendy (2007). Eva J. Nesselroth, Susan Cody: Genre, Narrative and the "Nigerian Letter" in Electronic Mail. Proceedings of the 40th Annual Hawaii International Conference on System Sciences HICSS 2007: 70

Cohen, Lawrence, and Marcus Felson (1979). "Social Change and Crime Rate Trends". American Sociological Review 44: 588. doi:10.2307/2094589.

Deborah, F. (2005) "Spam: How it is hurting e-mail and degrading life on the Internet," Deborah Fallows, Pew Internet & American Life Project.
<http://www.pewinternet.org/report_display.asp?r=102>;

Gbenga, S. (2007) The growing Menace of Cyber Crime in Nigeria- Causes, Effects & Solutions - http://events.tigweb.org/12657

Holt, T and Graves, D (2007) - A Qualitative Analysis of Advance Fee Fraud Email Schemes - International Journal of Cyber crime & Criminology 1(1)

Igwe, C (2007). Taking Back Nigeria from 419: What to do about the Worldwide E-mail Scam - Advance Fee Fraud (Bloomington: iUniverse).

Longe, O.B & Chiemeke, S.C. (2006): The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences. Pp 1 – 7. Covenant University, Ota, Nigeria. June, 2006

Longe, O.B, Chiemeke, S.C., Onifade, O.F and Longe, F.A. (2008): Text manipulations and spamicity measures: Implications for designing effective filtering systems for fraudulent 419 scam mails. African Journal of Information Technology Vol. 4 No. 3

Chiemeke, S.C and Longe, O.B (2008b): Shifting Paradigm In the Antispam Efforts – Outbound Filtering For Dealing With Nigerian Fraudulent Spam Mails. Journal of Computer Science and Its Applications Vol. 15, No 1

Olowu, D., 'Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa', 2009(1) Journal of Information, Law & Technology

Oriola, T (2005), 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response', 21(3) Computer Law & Security Review. Cardiff Law School UK

Peter et al (2006): Spamalot: A Toolkit for Consuming Spammers' Resources. CEAS 2006

Profgame Blogspot (2007) Smile out of Poverty – Cyber Crime in Nigeria – A Sociological Analysis: http://profgame.blogspot.com/2008/08/cyber-crime-in-nigeria-sociological.html

Reich, P (2004), 'Advance Fee Schemes in Country and Across Borders', International Connections, conference organized by Australian Institute of Criminology, Melbourne, Australia (Australian)

Ribadu, N. (2007) - Cybercrime and Commercial Fraud: A Nigerian Perspective. Congress to celebrate the fortieth annual session of UNCITRAL Vienna, 9-12 July 2007

Russell G. Smith (2001): Cross-Border Economic Crime: The Agenda for Reform Australian Crime Research Centre . Australian Institute of Criminology, Melbourne, Australia (Australian)

Tenfa, D (2006), Advance Fee Fraud (University of South Africa). (Thesis)

USIC3 (2009)- Internet Crime Complaint Centre Report (2006-2008). www.ic3.gov/media/annualreports.aspx

Tony, B. (2009): Gone Phishing http://netsecurity.about.com/od/secureyouremail/a/aa061404.htm