ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Prototype Scalable System for Secured Bulk SMS Delivery on Mobile Networks

Longe, O.B*
Int. Centre for Info Tech. & Dev.
Southern University
Baton Rouge, USA
longeolumide@fulbrightmail.org

Longe, F.A.
[2]Africa Reg Center for Inf. Science (ARCIS)
University of Ibadan
Ibadan, Nigeria
adefolakelonge@yahoo.com

Abdulrahman Abdulganiyu
Department of Math's/Computer Science
Ibrahim Badamosi Babangida University
Lapai, Niger State, Nigeria
Abdulg2009@yahoo.com

Adegoke, K
Department of Computer Science
University of Ibadan
Ibadan, Oyo State
Nigeria

Abstract - We developed a prototype scalable system for secured bulk SMS service delivery to assist in protecting unsuspecting users against social engineering attacks that cyber criminals use to harvest personal information on mobile networks. The system which is capable of interfacing with bulk SMS applications built using PHP and other scripting languages such as ASP, COLDFUSION and JSP interfaces with a decision engine which employs naïve bayes probability to classify messages and filter SMS message contents. When fraudulent messages are detected, it flags the network and take punitive actions against the user. It was developed using HTML tools and implemented using Object Oriented PHP, JavaScript and MySQL. The system is scalable and can be expanded for more enhancements.

***Keywords*:** SMS, Cyber crime, Cyber criminals, personal information, networks.

I. INTRODUCTION

Cyber criminals now explore bulk Short Message Service as an affordable means for victimizing unsuspecting users. Through social engineering tactics, they deceive mobile system users to part with access codes such as credit card number, ATM pin numbers, bank account details, social security number and other personal information. This development is inimical to the adoption of bulk SMS messages for genuine marketing, information provision and other promotional activities on service provider's network. The costs of these nefarious activities are borne by the public who lose huge amount of money as a result of these deceitful act and by Internet service providers who invest human and material resources into increasing bandwidth and storage space [14]. Short Message Service (SMS) is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile phone devices.

SMS text messaging is the most widely used data application in the world, with 2.4 billion active users, or 74% of all mobile phone subscribers. The term SMS is used as a synonym for all types of short text messaging, as well as the user activity itself, in many parts of the world [2]. SMS as used on modern handsets was originally defined as part of the Global System for Mobile Communications (GSM) series of standards in 1985 as a means of sending messages of up to 160 characters [3], to and from GSM mobile handsets. Since then, support for the service has expanded to include other mobile technologies such as ANSI CDMA networks and Digital AMPS, as well as satellite and landline networks. Most SMS messages are mobile-to-mobile text messages, though the standard supports other types of broadcast messaging as well [4].

SMS spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media such as instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. [5][2]. Spamming remains economically viable because advertisers have little or no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings [6].

II. RELATED WORKS

The idea of adding text messaging to the services of mobile users was latent in many communities of mobile communication services at the beginning of the 1980s. The first action plan of the CEPT Group GSM, approved in December 1982, requested "The services and facilities offered in the public switched telephone networks and public data networks... should be available in the mobile system" [4]. This target includes the exchange of text messages either directly between mobile stations, or transmitted via Message Handling Systems widely in use since the beginning of the 1980s [7]

This concept allowed SMS to be implemented in every mobile station, by updating its software. This concept was instrumental for the implementation of SMS in every mobile station ever produced and in every network from early days. Hence, a large base of SMS capable terminals and networks existed when the users began to utilize the SMS [8]. A new network element required was a specialized Short Message

Service Center, and enhancements were required to the radio capacity and network transport infrastructure to accommodate growing SMS traffic. SMS gateway providers facilitate SMS traffic between businesses and mobile subscribers, including mission-critical messages [9], SMS for enterprises, content delivery, and entertainment services involving SMS, e.g. TV voting. Considering SMS messaging performance and cost, as well as the level of messaging services, SMS gateway providers can be classified as aggregators or SS7 providers. The aggregator model is based on multiple agreements with mobile carriers to exchange 2-way SMS traffic into and out of the operator's SMSC, also known as local termination model [10].

The GSM industry has identified a number of potential fraud attacks on mobile operators that can be delivered via abuse of SMS messaging services. The most serious of threats is SMS Spoofing. SMS Spoofing occurs when a fraudster manipulates address information in order to impersonate a user that has roamed onto a foreign network and is submitting messages to the home network. Frequently, these messages are addressed to destinations outside the home network – with the home SMSC essentially being "hijacked" to send messages into other networks [12].

The only sure way of detecting and blocking spoofed messages is to screen incoming mobile-originated messages to verify that the sender is a valid subscriber and that the message is coming from a valid and correct location. This can be implemented by adding an intelligent routing function to the network that can query originating subscriber details from the HLR before the message is submitted for delivery. This kind of intelligent routing function is beyond the capabilities of legacy messaging infrastructure [13].

Mobile phone scam is becoming nauseating in Nigeria as it now forms an integral tool for advance fee fraud. It has become popular with the evolution of bulk SMS services in which the subscriber can brand the sender ID to send multiple messages to recipients. Scammers now brand their messages with network provider's names such as GLO, ETISALAT, ZAIN, MTN etc and send messages to recipients informing them that they have won huge sums of money and that they should call a particular number to claim their prizes. So many Nigerians have fallen victim of this singular act, thus creating a lack of trust in bulk SMS systems as a medium for disseminating information and contributes to consumers believing any authentic promotional activity being run by telecommunication companies.

III. RESEARCH DIRECTION

Bulk SMS scam remains poses a threat to the privacy of mobile phone users and cause most of the messages from legitimate businesses and marketers to frequently be lost in the deluge of utter crap that hits mobile phone users. It also makes legitimate Internet Service Providers (ISPs) to bear the costs because they have to spend money on increasing bandwidth and storage space caused by the escalating spam deluge. This burden is placed on users by spammers and by rogue ISPs and open relays that allow spam to flourish. Unfortunately, many bulk SMS providers in Nigeria have been shut down as they cannot control the flow of fraudulent messages through their web portal. Relatively, we can say SCAM messages have caused innocent citizens their jobs and integrity.

A. Existing SMS Filter Architecture:

Most of the local BULK SMS providers rely on their gateway providers to detect SCAM SMS messages and halt it from entering the SS7 link. Unfortunately, some SMS gateway providers do not have SPAM filters i.e MACH connectivity and RouteSMS. Since they do not have SPAM filters, these gateway providers are always careful with the traffic they are queuing up on the SS7 links worldwide. As a result of this, it becomes difficult for local providers to connect their websites to these service providers as they cannot guarantee the safety of their traffic (i.e. a SMS traffic void of SCAM messages).. This architecture is summarized in fig. 1

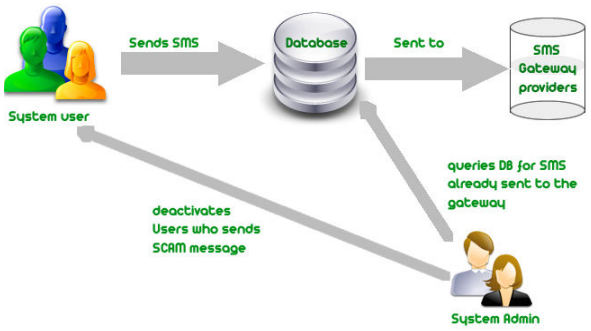

Figure 1: Architecture of the Current System

What local SMS providers offer as a valve to prevent SMS scamming is the use of manual sorting method to identify scam SMS. They normally employ the service of a manager who goes through messages sent on the BULK SMS sites and manually deactivates the user sending SCAM messages. This method is crude and relatively ineffective. This is because a message sent by the system user would have gotten to the recipient before an admin gains access to the system. The admin can only deactivate a user sending SCAM, unfortunately registration is free thus the deactivated user can re-register using another set of credentials. The current system is faulty as it only allows an administrator to deactivate the system users. It does not block / disallow system users from sending the SCAM message.

B. Proposed Architecture:

The need therefore arise to develop a new system that can automatically scan through SMS messages and determine whether they are spam or not and then take necessary actions. We propose an architecture that will SCAN through every message that is about to be sent to the SMS gateway providers using Naïve Bayesian probability to identify and classify scam messages. The advantage of Bayesian spam filtering is that it can be trained and can learn on a per-user basis since most user receives spam messages that are related to their activities (personalized) [14].

The application will be capable of updating itself from the repository of newly invented SCAM words in order to handle concept drift. It will then determine whether the message is spam or not. If it is spam, the user is deactivated and the message is added to the repository of Scam messages. This system will be provided as an add-on or

plug-in (as the case may be) to existing gateways as an aid to detecting fraudulent SMS messages in Nigerian BULK SMS websites. The diagram on the next page shows an overview of the new proposed system.

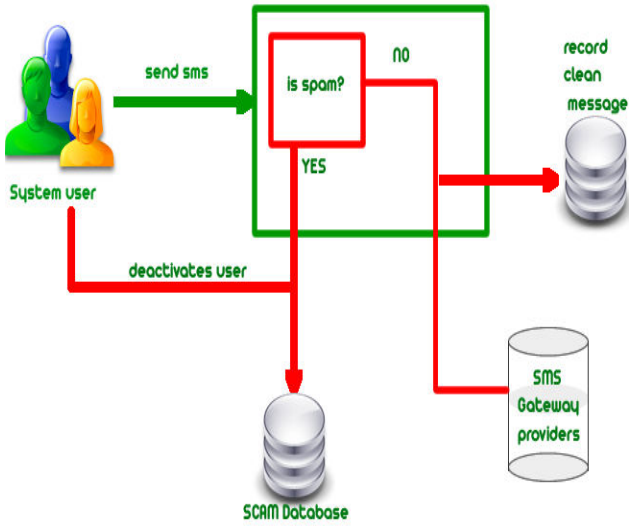

Figure 2: Architecture of the Proposed System

C. *Computing Spam cities:*

Bayesian email filters take advantage of Bayes' theorem. Bayes' theorem is used several times in the context of spam filtering [11].

a. A first time, to compute the probability that the message is spam, knowing that a given word appears in this message;
b. A second time, to compute the probability that the message is spam, taking into consideration all of its words (or a relevant subset of them);
c. A third time, to deal with rare words.

To compute the probability that a message containing a given word is spam, the system employs the Bayes' theorem using

$$\Pr(S|W) = \frac{\Pr(W|S) \cdot \Pr(S)}{\Pr(W|S) \cdot \Pr(S) + \Pr(W|H) \cdot \Pr(H)}$$

.....(1)

where:

$\Pr(S|W)$ is the probability that a message is a spam, knowing that the word "replica" is in it;

$\Pr(S)$ is the overall probability that any given message is spam;

$\Pr(W|S)$ is the probability that the word "replica" appears in spam messages;

$\Pr(H)$ is the overall probability that any given message is not spam (is "ham");

$\Pr(W|H)$ is the probability that the word "replica" appears in ham messages.

The spamicity (or spaminess)

Statistics generally reflect that current probability of any message to be spam is 80%, at the very least

$$\Pr(S) = 0.8; \Pr(H) = 0.2$$

However, most Bayesian spam detection software make the assumption that there is no a priori reason for any incoming message to be spam rather than ham, and consider both cases to have equal probabilities of 50%:

$$\Pr(S) = 0.5; \Pr(H) = 0.5$$

The filters that use this hypothesis are said to be "not biased", meaning that they have no prejudice regarding the incoming email. This assumption allows simplifying the general formula to:

$$\Pr(S|W) = \frac{\Pr(W|S)}{\Pr(W|S) + \Pr(W|H)}$$

.....(2)

This quantity is called "spamicity" (or "spaminess") of the word "replica", and can be computed.

D. *Combining individual probabilities:*

The naivety of the Bayesian spam filtering system is experimented when it makes the assumption that words present in the message are independent of one another (Longe, 2009) and thus derive another formula from Bayes' theorem:

$$p = \frac{p_1 p_2 \cdots p_N}{p_1 p_2 \cdots p_N + (1-p_1)(1-p_2)\cdots(1-p_N)}$$

.....(3)

where:

p is the probability that the suspect message is spam;

p_1 is the probability

p(S | W1) that it is a spam knowing it contains a first word (for example "replica");

p_2 is the probability

p(S | W2) that it is a spam knowing it contains a second word (for example "watches");.

pN is the probability

p(S | WN) that it is a spam knowing it contains a Nth word (for example "home").

The result p is usually compared to a given threshold to decide whether the message is spam or not. If p is lower than the threshold, the message is considered as likely ham, otherwise it is considered as likely spam.

E. *Handling Spurious and rare Words:*

In the case a rare word with which the spam filtering engine has not been trained, the numerator and the denominator equals zero for the general formula and in the spamicity formula. The software discards such words for which no information is available Words rarely encountered when training the filtering engine can rarely be trusted as they contribute less to the efficiency oif the filtering engine. They are better discarded in computing spamicity. One and two letter words sucs as “it” “on”, “if”, “im” and “no” hardly contribute anything to the efficiency of spam filters. They are also discarded. In this case, corrected probability is used and the formula below is adopted.

$$\Pr'(S|W) = \frac{s \cdot \Pr(S) + n \cdot \Pr(S|W)}{s+n}$$

where:

$\Pr'(S|W)$ is the corrected probability for the message to be spam, knowing that it contains a given word ;

s is the strength we give to background information about incoming spam ;

$\Pr(S)$ is the probability of any incoming message to be spam ;

n is the number of occurrences of this word during the learning phase ;

$\Pr(S|W)$ is the spamicity of this word.

$\Pr(S)$ can again be taken equal to 0.5, to avoid being too suspicious about incoming email.

$\Pr(S)$

IV. SYSTEM DESIGN

The basic functional requirements include the design of a token database of the various tokens used by Spammers when sending their messages. It will be a continually expanding database because Spammers come up with new and different words in order to deceive people. An SMS Spam Filter Service is needed to ensure that SMS sent to the gateway providers are void of SCAM text. The filter must be flexible to suit the local provider's needs and tailored to solving the problem of flooding and illegal spoofing. The anti-spam service should also provide the following services

a. Ability to automatically deactivates a user who sends SCAM message
b. Ability to train itself with the newly detected fraud message.
c. Ability to detect IP address of the source message and blacklist as appropriate
d. Ability to also Whitelist IP addresses and users.

The spam filter service should also allow the user to allow a message to join the SS7 link in case of false positives. An SMS API – anti SPAM service is needed since most of the bulk SMS applications existing were developed with PHP. Since the syntax of other scripting language such as ASP, Coldfusion and JSP differs, it becomes imperative to develop an interface through which these websites developed in different languages can interface with the anti–Scam database and determine whether the message is Scam is not. The API will accept inputs such as message, sender ID, IP address etc and in turn return a single response-whether the message input is spam or not.

In our architecture, the bulk SMS buyers can do the following

a. Create an account
b. Login to his/her personalized account
c. Request for a change in password if the old one is forgotten
d. Send SMS (to GSM numbers)
e. View/check SMS logs

Local bulk SMS providers can
The local providers can do the following

a. Control the percentage of control for the SCAM filter
b. Activates a client in a case of false positives
c. Allow a message to queue up on the SS7 link in the case of false positives.
d. Remove/ Whitelist IP address in case of false positives.
e. View the SCAM record of each user on the system
f. Deactivates a user in case of anti-spam failure.
g. Login

The anti-SMS Scam filter will be capable of doing the following.

a. Divide message into tokens
b. Determine the spamicity of each tokens
c. Determine the overall spamicity of a message
d. Determine whether a message is scam or not.
e. Ability to train itself with a spam message.

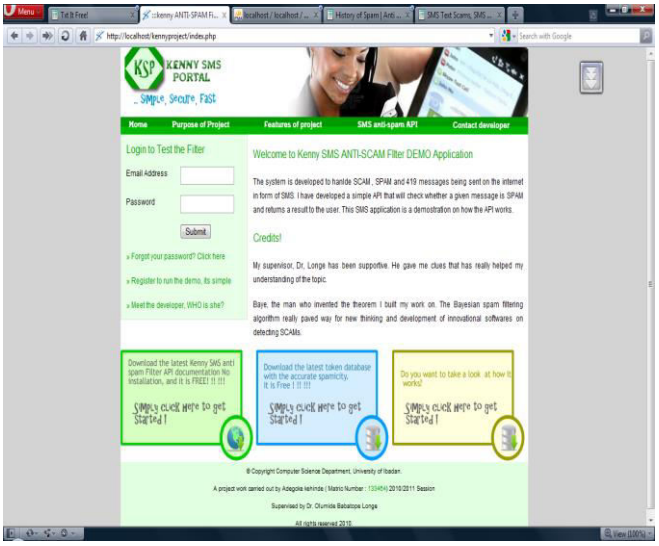

Figure 3: The homepage of the SMS SPAM detector Demo.

When the user successfully logs into the system, he/she is redirected to the Send SMS page. The send SMS page is a simple interface that allows user to type their messages and also spoof the sender ID. The SPAM detector has been plugged to the page and thus, before a message is being sent out to the recipient, the message is passed through the filter. The filter sieves it. If the message has a spamicity greater than 0.50, the message is tagged spam. The user's credit is also deducted and a report is displayed for the user to see the reason why the message could not be sent. If the user feels that the message is not SPAM, he/she can contact the administrator with the error number for the admin to check. According to report of test, almost all the messages caught by the newly developed filter is SPAM.

The next snapshot shows a typical Spam message that is about to be sent.

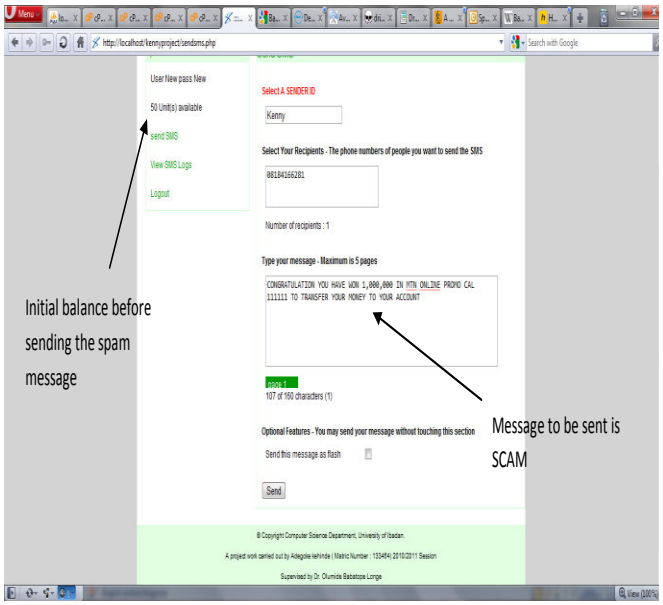

Figure 4: Typical SCAM message

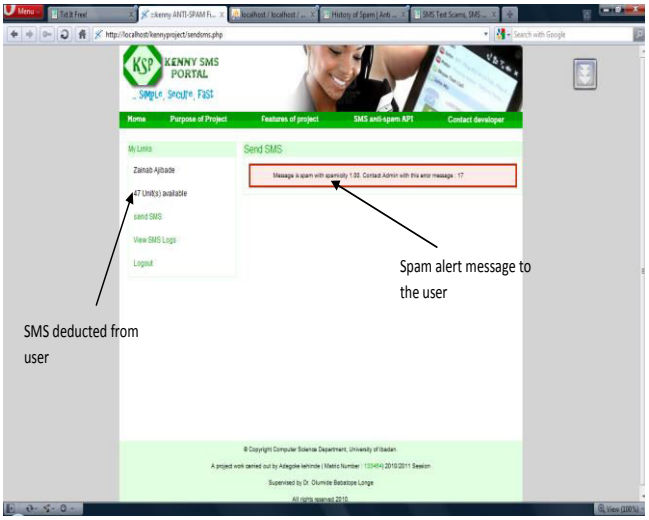

Figure 5: Typical Message not Sent

The sender Id and the message body are screened by the SPAM detector. If any one of them is greater than 0.50, the message is flagged as SPAM.

A. SMS logs:

Every user on the system is entitled to view the messages they have sent in the past. The logs display to the user the messages being sent.

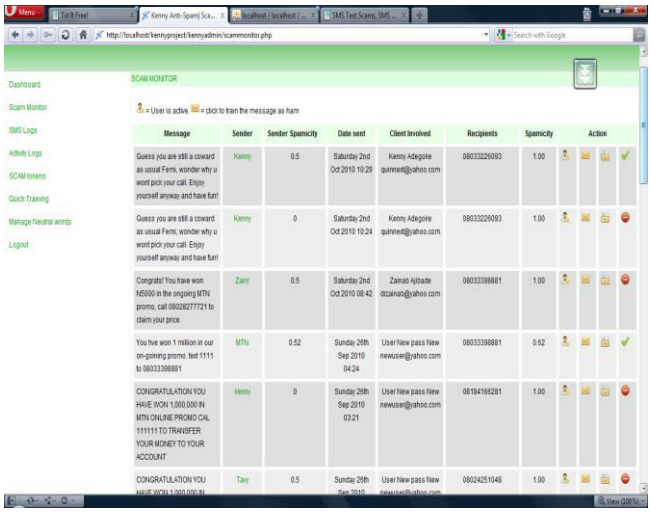

Figure 6: SCAM monitor

The scam monitor page displays to the admin every message that the SCAM detector identified as SCAM. The messages are displayed under the following heading.

Table: 1

Message	This is the actual message sent
Sender	This is the sender ID used when the message was sent
Sender Spamicity	The spamicity value of the sender ID used
Date Sent	The date the message was sent
Client Involved	The client who sent the scam message
recipients	The recipients the message was intended for
Message Spamicity	The spamicity of the message
Actions	This is shown when the user is active This is shown when a message has been used to train the scam detector This icon indicates that the admin can train a particular message as HAM this icon shows that a message is still available to be used to train the detector this icon indicates that the admin can train the detector as SPAM this icon indicates that the user has been blocked from using the system

By clicking on the sender, the admin can also spam the sender. This is because often times, some of this spammers test by first spoofing the Telecoms Company's brand name and so on.

V. CONCLUDING REMARKS

With the use of bulk SMS as a cheap means for information dissemination, internet criminals are also exploring this tool to defraud unsuspecting users by sending to them messages that mislead them to part with personal information. We have developed a filter for bulk SMS web applications. This filter disallow fraudulent messages from getting to intended recipient and at the same time takes appropriate measure on the perpetrator. The SCAM detector is built as an API that any bulk SMS service provider can use to check the spamicity of their messages, irrespective of the platform of implementation of their bulk SMS application. The intention is to make mobile platform more secured for service providers and operators and increase user confidence in mobile technologies.

VI. REFERENCES

[1] Writeservice (2011) Spam and its ill effects. http://www.writersservices.com/www/v_joe_job.htm (1)

[2] M. Sahami, S, Dumais, D.Heckerman, & E. Horvitz). "A Bayesian approach to filtering junk e-mail". AAAI'98 Workshop on Learning for Text Categorization. 1998. pp 55-62. (2)

[3] MozillaZine."Junk Mail Controls" November 2009

[4] Word Spy – Ham:
http://www.wordspy.com/words/ham.asp

[5] Advance Fee Fraud – Paying money for a promise of wealth (419 Fraud)
http://www.met.police.uk/fraudalert/419.htm

[6] O.B. Longe, S.C. Chiemeke, O.F.W. Onifade & F.A. Longe. "Camouflages and token manipulations: The changing faces of the Nigerian fraudulent 419 spammers. African Journal of Information Technology,. 2008 Vol 4 (3), 87-98.

[7] M. Dylan & H. Dermot. "State of Spam, a Monthly Report - Report #33". Jan. 2009

[8] R. Gary "A statistical approach to the spam problem". The Linux Journal. 2003.
http://www.linuxjournal.com/article/6467

[9] Internet Society's Internet Engineering Taskforce. "A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam)".2012.
http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force

[10] Spamming? (rec.games.mud) - Google Groups USENET archive, 1990-09-26

[11] Braver v. Newport Internet Marketing Corporation et al. -U.S. District Court - Western District of Oklahoma (Oklahoma City), 2005-02-22

[12] Wired Magazine."The (Evil) Genius of Comment Spammers" Wired Magazine, March 2004

[13] R. J. William. "Thank the Spammers". 2003. ww.linxnet.com/misc/spam/thank_spammers.html

[14] Tom. "A very unhappy birthday to spam, age 30". 2008. San Francisco Chronicle.

http://streetknowledge.wordpress.com/2008/06/02/how-many-sex-partners-have-you-really-had/