ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (76-79), Month: April - June 2018, Available at: www.researchpublish.com

E-Policy for Spam Mail

[1]Musa Bala Shuaibu, [2]Abdulkareem Al-Alwani

[1,2]Department of Computer Science and Engineering, Yanbu University College, Yanbu Industrial City, Saudi Arabia

Abstract: **There are more than 13 billion of unsolicited emails that are sent around the world each day which amounts to about $14 per user per month in terms of productivity lost to companies around the world. This is as a result of inconsistencies in the global laws on spam emails. This paper proposes an e-policy that will restrict and protect data regarding sending and receiving spam both external and internal.**

Keywords: **E-Policy, Spam Mail, Data Protection, Mailing List.**

I. INTRODUCTION

The introduction of paper contains the nature of research work, purpose of work, and the contribution of this paper. It contains the references of the previous work done. This template is in Word document, provides authors with most of the formatting specifications required by the author for preparation of their As email is becoming part of daily life of people, there is a great concern due to the wide spread abuses of spammers who send massive unsolicited mails targeting collection of address list which were from various sources. Spam mails refer to sending inappropriate or unsolicited messages to recipients for the purpose of advertisement, fraud or other cybercrime. Due to the fact that the act of spamming the bulk of these messages are sent anonymously with no costs, legitimate email messages are been thwarted.

The main reasons why spamming became facilitated is firstly because many users after visiting a site provide the site with their email address in order to open an account or join a news group which makes available the collection of large email addresses from the users.

There is also the reason that due to absence of policy in respect to the mailing list such that on one hand, users are not restricted to what mailing list they can subscribe to, while on the other hand any individual has the right to post whatever to anyone. This opens the doors for the world to keep sending spamming mails at no cost.

There is also the notion that most a times, organizations do not have a categorization envelope where spam mails will be distinguished from genuine emails. The users need to first open the message before sending it to spam folder.

According to [1] the estimated figure for spam messages is around seven seven trillion which includes the cost involved in lost productivity and fraud, and extra capacity needed to cope with the spam. It has been identified that between 88 – 92% of email messages sent in the first half of 2010 carried spam. Figure 1.0 shows the relative proportions of the types of malware samples send in form of spam.

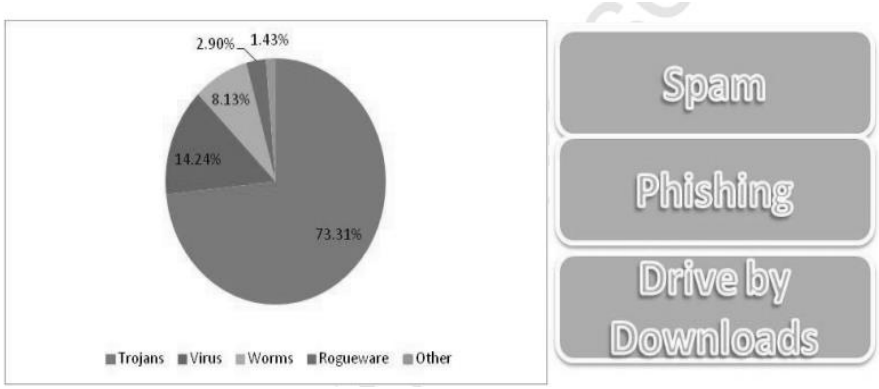

Figure 1: Malware send as spam [1]

Although there are prevention and detection methods propounded by practitioners in this domain, these methods are mostly time consuming or expensive which became very crucial for an inexpensive methods to be in place. It is also a known fact that there have been some high profile convictions, but the focus is therefore not on technological algorithms to directly prevent spammed.

II. RELATED WORKS

Despite the prevention and control methods, spammers continue to cost businesses revenue loss in millions of dollars which calls for the need for legislation at both global and organizational level to combat spam.

According to [2], there is need for consistent laws around the world otherwise cubing spam emails will not work without a global tie-up in legislation because it is a global problem and needs a global solution,

Countries such as Singapore enacted legislation to response to the exponential growth of spam in an integral way that form part of her multi-faceted approach to this worldwide problem. The country proposed Spam Protection Act refers to as Legislative Framework for the Control of E-Mail Spam[3]. The act aims not to eradicate all unsolicited commercial electronic messages but only those defined as spam. It seeks to balance the legitimate use of e-mail as a cost-effective marketing tool for e-Commerce with the protection of end users and Internet Service Providers (ISPs).

Other policies were drawn upon the legislative experience of the UK, USA, Australia, Japan and South Korea, which uses validation on messages send by senders domain specified in the "MAIL FROM:" address of the message envelope. For example, when a mail from paypal.com requests revalidation of users' account and password, the validation checks if it is sent from the domain paypal.com or is part of a scam [4].

In Saudi Arabia, the Communications and Information Technology Commission CITC is charged with regulating the telecommunications sector in the Kingdom. It oversees the application of the Telecommunications Act, its Bylaw and the Ordinance of the CITC. CITC promotes the establishment of Commercial Secure Mail which host providers who receive e-mails on behalf of companies and filter them before delivering them to the mail servers of the companies[5] .

III. MACHINE LEARNING FILTERS

Machine learning algorithms are used for anti-spam paradigm in order to filter spam email messages based on identified training and testing similarity. The procedure enables learning of patterns associated with the flagged spam email and turns out to be more accurate and precise than when a user will do it manually. Machine learning approach could be an unsupervised learning techniques which are set of classification algorithms described as artificial intelligence fields[6] or the supervised. Therefore, There are various machine learning algorithms identified in this review which include Naïve Bayesian, Neural Networks[7] artificial neural network[8] memory based, pattern discovery, case based, Greylisting, SMTP path analysis, trust network Term.

A. Non-Machine Learning Filters:

In contrast, non-machine learning filters include heuristics, signatures, blacklisting, hash based, traffic analysis etc are based on methods that list some keywords as spam emails. The methods are subject to constant manual update in order to catch the latest spam. For example [9] using the non-machine learning to filters spam. However in recent years, machine learning and hybrid paradigm are the more frequently used paradigms, probably due to the fact that spammers keep improving their techniques for sending spam messages over time, which makes it more complicated for heuristic and other non-machine learning techniques to detect and prevent. Despite that, machine learning paradigms may not be an alternative for non-machine under conditions where spam emails are changing in their nature.

B. E-policies for Spam:

Based on a review conducted on spam policy globally and within organizations, we proffer some e-policies that has to do with handling spam by users or employees which will assist in combating spam. The E-policies specify how employees should handle unsolicited e-mail, especially if the e-mail contains offensive material. The reason behind our e-policy is that, in the absence of e-policy in an organization, users have the right to post messages of whatever content to anyone and also users can subscribes to any un-moderated mailing list which may invite spammers from all over the world into the organization. The consequence of such act is that, spam of such subscribed list tends to be extremely hard to remove from the domain. Though automated filters are put in place to check unsolicited spam mails, the filters become inefficient if the spam comes as a whitelist for the individuals who subscribe to the mailing list.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (76-79), Month: April - June 2018, Available at: www.researchpublish.com

Therefore, we provide the following policies with respect to the senders:

a. When submitting personal information online to websites, chart rooms or news group, users or employees must ensure that they carefully read the privacy policy that governs how that personal information will be handled and the opting-out policies.

b. Receiver authentication is another significant e-policy that must be observed. The receiver of an e-mail should authorize whether such email address is legitimate and hence be added to the whitelisted email addresses of the organization. This will transfer the authorization of whether an email is spam or not to the receiver of the email and hence reduce the risk of blocking other legitimate emails from reaching the intended recipients (fig 2).

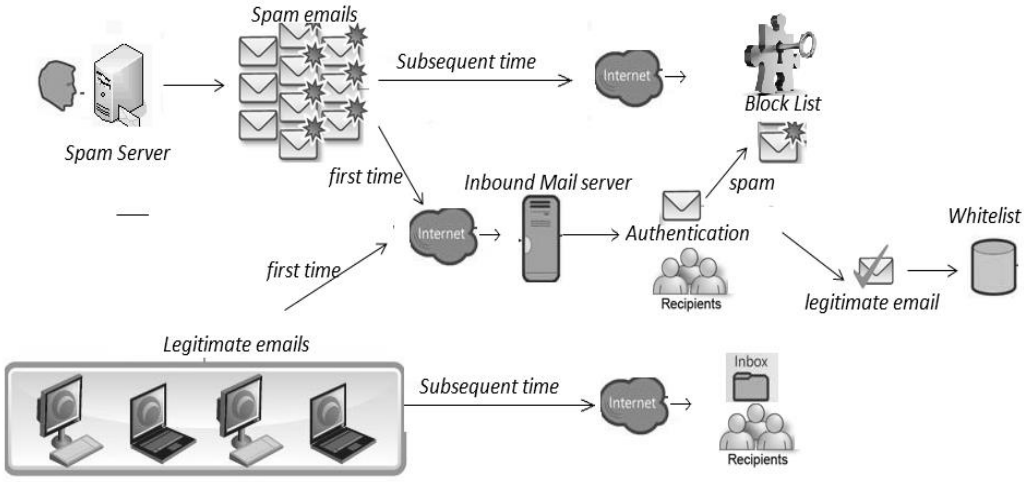

Fig 2: Recipient Authentication Policy

c. In case of an unsure or concern message, users must seek the attention of a superior manager to discuss the legitimacy.

d. Users must not necessarily reply an email just to inform the sender that he has received the email.

e. Users should not use 'message delivered' tracking unless when it is absolutely necessary because it generate significant email traffic.

f. When replying to emails received, use a portion of the original message send to reply.

g. Users should cultivate the habit of discarding all un-important messages to avoid too long messages.

IV. CONCLUSION

As long as spamming continues to be profitable because of the very low marginal cost of sending bulk e-mail and the availability of sophisticated automated spamming tools, indiscriminate mass mailing is likely to continue if organizations do not vigorously embrace tough spam laws. The enforcement is beyond the ambers of private and business individuals without the involvement of all stakeholders.

REFERENCES

[1] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, pp. 973-993, Aug 2014.

[2] H. Shahriar and M. Zulkernine, "Mitigating program security vulnerabilities: Approaches and challenges," ACM Computing Surveys (CSUR), vol. 44, p. 11, 2012.

[3] Everett, "Stronger laws needed to stem spam," Computer Fraud & Security, vol. 2004, pp. 1-2, 2004.

[4] T. K. Leng, "Singapore's multi-pronged strategy against spam," Computer Law & Security Review, vol. 22, pp. 402-408, 2006.

[5] S. Görling, "An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism," Internet Research, vol. 17, pp. 169-179, 2007.

[6] M. A. Al-Kadhi, "Assessment of the status of spam in the Kingdom of Saudi Arabia," Journal of King Saud University-Computer and Information Sciences, vol. 23, pp. 45-58, 2011.

[7] A. Al-Alwani, "An Investigation of the State of the Art in Spam Email Detection and Prevention Indicating Future Research Directions," International Review on Computers & Software, vol. 7, 2012.

[8] J. B. S. Dhifallah, et al., "Classification Methods Based on Pattern Recognition and on Neural Networks for Failure Detection," International Review on Computers & Software, vol. 5, 2010.

[9] M. Mirdehghani and S. A. Monadjemi, "Aesthetic Evaluation of Web Pages Using Texture/Color Features and Artificial Neural Networks," International Review on Computers & Software, vol. 4, 2009.

[10] M. Soranamageswari and C. Meena, "A novel approach towards image spam classification," International Journal of Computer Theory and Engineering, vol. 3, pp. 84-88, 2011.