Possible Decrease of Spam in the Email Communication

K. Šolić*, D. Šebo*, F. Jović ** and V. Ilakovac*
* Faculty of Medicine, Osijek, Croatia
** Faculty of Electrical Engineering, Osijek, Croatia
kresimir@mefos.hr

Abstract - The problem of spam has great impact on the Internet users, it questions safety and usefulness of the use of electronic mail, its cost and time consuming, as well as the effectiveness of the Internet in general.

In this work authors analyze cost of spam and its law regulations (in Croatia and Europe) and with case report and simulation they are trying to answer several questions: is there decrease of spam in last few months and what are possible reasons; is there more spam because of the users' risky behaviour; is there more spam because email addresses are put on a web site; is email user obligated to receive spam; is there more unwanted mail on free world-wide known email services?

Most of the nowadays research on this subject gives algorithms and software solutions as new improved spam filters, but this work analyses users' behaviour and different regulatives. As there are law regulations and technical solutions like spam filters on both users' and providers' side attention should be paid to users' behaviour and their awareness on how to ignore spam and by doing this to suppress spam in the longer period of time.

I. INTRODUCTION

It is practice to define the term "spam" as the "unwanted and unsolicited electronic mail", that has usually (though not necessarily) been sent to many recipients. Although the problem of spam is growing continuously, it actually preceded the existence of the Internet. One of the first cases of spam was in 1978, when Digital Equipment Corporation (DEC), in that way, sent messages to the ARPAnet and promoted their products [1]. The problem of spam has a great impact on Internet users, it questions safety and usefulness of the use of electronic mail, its cost and time consuming, as well as the effectiveness of the Internet in general.

In this work authors analyze cost of spam and its law regulations (in Croatia and Europe) and with case report and simulation they are trying to answer several questions:

- Is there less spam in last few months and if so what are possible reasons [2],
- Is there more spam because of the users' risky behaviour (e.g. registration on different sites) [3],
- Is there more spam because email address is put on the web site [4],
- Is even a careful email user obligated to receive spam,
- Is there more unwanted mail on free world-wide known email services like Gmail, Yahoo and Hotmail which are more compromised and less secure than institutional email addresses and Croatian ISP's email services [5-9]?

Most of research on this subject gives software solutions as new improved spam filters, but this work analyses users' behaviour and different regulatives. As there are law regulations nowadays and technical solutions like spam filters on both users' and providers' side attention should be paid to the users' behaviour and their awareness on how to suppress spam [10]. As it is not just ICT's problem, companies/institutions should define security policies [11-13].

II. ECONOMICS OF SPAM

Spamming is a lucrative business in which it is possible to earn millions of Euros. To understand how such a generally unwanted operation can be so successful, one must look into the economics of spamming. The economics of spam can be divided into a number of topics [14]:

- Cost and revenues of spamming,
- Distorted costs, or negative extra lines of spamming,
- Beneficiaries of Spamming.

A. Costs of spam

The fixed costs for spammers are relatively low. Even a desktop PC can generate large volumes of email messages. The cost of generating one more email once the basic equipment and network services are in place is virtually nothing. The result is that the low cost of spam allows spammers to supply large volumes of spam.

Second factor is that even though a spammer might send out million messages, only a small fraction, for example 100 recipients, might respond. Those 100 respondents actually pay the price that covers the cost and profit for the spammer. Although most consumers do not respond to any spam, a small number of consumers responding to even a fraction of all spam they receive can sustain the economic motivation for spamming.

B. Cost of spam incurred by others

Business and other organizations incur costs related to spam. These costs could be divided as follows:

- Wasted bandwidth,
- Load on email services,
- Disk and archival storage,
- Anti-spam applications,
- Employee's time.

According to research conducted in the European Union the amount of spam (measured both in quantity and bandwidth) has grown [15]. Recent studies report that almost 90% of all email traffic is considered spam [16]. The amount of spam sent from EU countries is also increasing. At the same time, less spam reaches users' mailboxes, showing that providers have invested considerably in protecting their customers from spammers in their own networks.

Spam also places additional storage load on email servers. If an organization does not want to risk deleting legitimate email, it might choose to store and archive all emails, including spam. The additional storage and archival costs are born by the recipients of spam, not the senders.

C. Anti-spam law

On 25th June 2002, the Council of the European Union formally adopted the Electronic Communications Privacy Directive, also known as Directive 2002/58/EC of the European Parliament and of the Council [17]. This Directive is the basis for the anti spam laws of all the EU member countries. Unlike EU Legislation which is immediately binding on member nations, a Directive requires that each member nation introduce their own anti-spam legislation compatible with and reflecting the EU Directive.

Some of the Major Provisions of the European Union Spam Law:

- The directives cover not only email spam, but also spam sent via SMS and MMS,
- Applies to all electronic communications received by or sent from networks in the European Union ,
- The definition of spam does not specify quantity. It appears that, in particular circumstances, a single email may constitute spam,
- It also introduces restrictions on the use of cookies (more a privacy issue than a spam issue, so we will not elaborate on that here),
- The Directive takes an "opt-in" approach, making illegal the sending of commercial email without prior consent of the recipient,
- Some commercial email is permitted without an explicit opt-in in certain specific circumstances (implied-opt-in, or soft-opt-in),
- It is unlawful to disguise or conceal the identity of the sender,
- Every email must include sender's name and return address,
- Every email must provide clear, working opt-out instructions and opt-outs must be free of charge.

In Croatia there are no specific laws on spam, there is only Law on Telecommunications from year 2003 where only two articles could be found that touch on the spam [18]. Specifically, Article 111 which defines what is considered spam or unwanted telecom communications and the conditions under which and how such communication can be sent, while Article 116 brings penalties for violators.

Law is one basis for spam suppression, meaning arrests of spammers and hackers [19].

III. CASE REPORT

On the official web site of the Croatian Society for the Medical Informatics (HDMI) there is sub site on the symposium „Medicinska informatika 2009". For the registration and official communication with the organising committee there was an email address highlighted on this web site [20].

Analysis of the regular and spam mail received on this email address was made through the period of two years (Fig.1.). This two time series show the amount of the regular email versus spam through 23 months. Date 12th of December 2008 is the starting time stamp, the day when the first mail was sent (testing mail sent by the president of the organising committee to the other members of the committee). All interesting time stamps are:

- 12th of December 2008 - first email sent, test mail,
- 23rd of March 2009 - first official (regular) mail, registration to the symposium,
- 14th of February 2009 - first unwanted (spam) mail received,
- Symposium lasted from 8th till 9th of May 2009,
- 17th of September 2009 - last official (regular) mail received,

Today spam is still coming to that email address even though this email address has not been in use for more than a year.

IV. SIMULATION

Simulation was conducted with two basic premises. First one was that there will be more unwanted mail because of the email user himself being not careful with its email address (registering on different sites and leaving email unmasked on the web pages). Second premise was that even careful email user is sometimes obligated to receive spam.

Simulation period started at 1st of March and lasted till the end of the year 2010; and one of its aims was to find differences in amount of unwanted email messages received to the email addresses used in different ways. Four groups of email addresses were opened and used in different ways, as follows:

- First group is called "Web Group" which had 12 email addresses that were put on the web site [21],

- Second group is called "Registration Group" which had 18 email addresses used for all kind of registrations on Internet,
- Third group is called "Common Group" which had 17 addresses used for the regular/usual email communication,
- Last group is called "Control Group" which had 18 addresses that were opened but never used.

The "Web Group" was made of email addresses listed on the web page made for this purpose. Syntax was the true email address with active link in order to be found by spammers scanning the Internet for the addresses. However links to this web page and the registration to the Google search engine were made nine months later (during last days of November). A month later web page became searchable in Google.

With email addresses from the "Registration Group" authors were registering approximately every second week of the simulation period to different kind of web sites, like investment organizations, web-shop sites, forums, torrent sites, etc.

Email addresses from "Common Group" were used approximately every second week of the simulation period as personal addresses in personal send/receive email communication with real email users.

Last group of email addresses the "Control Group" was not used in any way. This group was for control purposes only, in case there was spam received on one of these email addresses it would mean that there is some kind of a problem with that domain (e.g. hacked email server, stolen back-up, etc.).

V. RESULTS

As expected, in the "Control Group" there was no spam received during whole period of simulation; however in the "Common Group" there was also no spam received during the same period. Amount of spam received in "Registration Group" and in "Web Group" is listed in the table below (Table I). Difference between domains was found statistically significant (more spam in the .com domain, p=0.043, Mann-Whitney U Test), but difference between groups was not statistically significant (p=0.518, Mann-Whitney U Test).

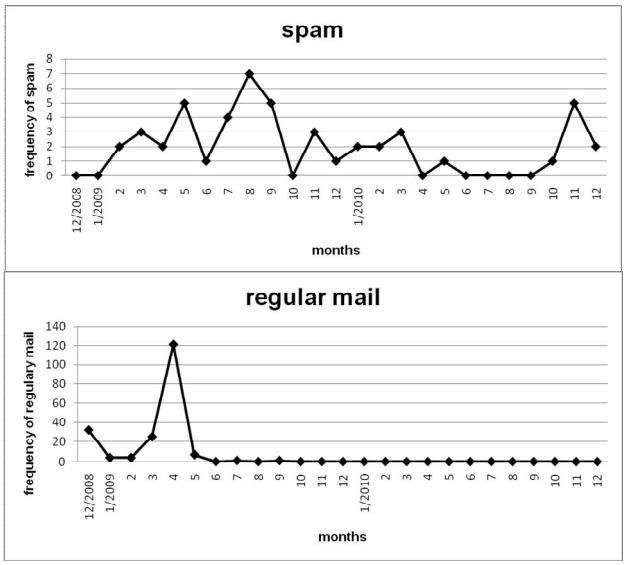

Fig. 1. Absolute frequency of spam and regular mail per month received on conference email address.

TABLE I. MEAN NUMBER OF SPAM RECEIVED

Email categories*	Differently used email groups		
	Registration Group (mean)	*Web Group (mean)*	*Mean of total*
Free email services (.com domain)	9.71	8.14	8.93
Croatian ISPs and institutional email addresses (.hr)	2.27	5.60	3.31
Mean of total	5.17	7.08	

* Based on security level [5]

The majority of spam was received in last two months of the simulation period, in November and December (after registering web site on Google search engine and posting addresses from the "Registration Group" on forums).

VI. CONCLUSION

Results of the simulation confirm first premise that there will be more unwanted mail because the email users were not careful with their email addresses, i.e. if address is used for frequent registrations, left on web sites or forums. However second premise, that even careful email user is obligated to receive spam, was not confirmed as authors did not get any unwanted mail to any of the email addresses included in the "Common Group".

Amount of spam received to the conference email address during two-year period was low (Fig.1.). In the period of 25 months, maximum of 7 unwanted messages was received during August 2009 and for the following 8 months there was no spam at all. However, this is email address that has not been in use for 18 months but is still receiving some spam.

During the simulation period of 10 months amount of spam received was also, unexpectedly, low. Maximum of 22 unwanted messages during one month was received by only one email address in the last month of the simulation period, in the December. That is much and it is evident that spam still exists and is still a problem, but average of 5.17 or 7.08 unwanted messages received through mail system per month is small price for using email address on the Internet without caution (frequent registrations, email address highlighted on the web sites, forums, etc.).

It was expected that there will be more spam in email addresses of the free world-wide known email services (.com domain) than on the institutional and Croatian ISP's email systems (.hr domain). This is true in both "Registration Group" and "Web Group" (Table I).

However, withdraw of this study may be the short simulation period, but observing the case report it looks

like there is maybe less spam in the email communication nowadays. This may mean less spam in users' inboxes, but not less spam sent by spammers.

There are three possible components where suppression of the spam is possible: law regulations should suppress behaviour of spammers, software (filters and encryption) solutions are technical component and careful behaviour of users should be met by informing and education.

More attention should be paid to the last component, to the users' behaviour [3, 10, 22 and 23].

REFERENCES

[1] B. Templeton, "Reaction to the DEC Spam of 1978", availabe at: http://www.templetons.com/brad/spamreact.html (accesed December 2010).

[2] State of Spam & Phishing - A Montly Report, Symantec, available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf (accessed January 2011).

[3] The 25 Most Common Mistakes in Email Security, ITSecurity [available at: http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/ (accesed on Mart 2010).

[4] G. Schryen, "The impact that placing email addresses on the Internet has on the receipt of spam: An empirical analysis", computers & security, vol. 26, 2007, pp. 361-372.

[5] K. Solic, K. Grgic, D. Galic, "A Comparative Study of the Security Level among Different Kinds of E-mail Services - Pilot Study", Teh vjesn - Stroj fak. vol.17, No.4, 2010, pp. 489-492.

[6] P. Noiumkar, T. Chomsiri, "Top 10 Free Web-Mail Security Test Using Session Hijacking", Proc IEEE ICCIT, 2008, vol. 2, pp. 486-490.

[7] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions", TechChrunch, available at: http://techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/ (accesed on May 2010).

[8] F. I. Sullivan, "Wandered Lonely as a Cloud", Comput Sci Eng. IEEE.2008, vol. 88, pp. 1521-9615.

[9] L. Demer, "Governor's two e-mail accounts questioned", Anchorage Daily New, available at: http://www.adn.com/2008/09/14/526281/governors-two-e-mail-accounts.html (accessed on August 2010).

[10] K. Solic, V. Ilakovac, "Security Perception of a Portable PC User (The Difference Between Medical Doctors and Engineers): A Pilot Study" Med Glas Ljek komore Zenicko-doboj kantona, 2009, vol.6, No.2, pp. 261-264.

[11] J. VanderMeer, „Seven Highly Successful Habits of Enterprise Email Managers: Ensuring that your employees' email usage is not putting your comapny at risk", Information Systems Security, December 2006, pp. 64-75.

[12] E.G. Park, N. Zwarich, "Canadian government agencies develop e-mail management policies", Int J Inform Manag. 2008, vol.28, No.6, pp. 468-473.

[13] Information security standards, ISO, available at: http://www.iso.org/iso/specific-applications_it-security (accessed on December 2010).

[14] D Sullivan, "The Definitive Guide to Controlling Malware, Spyware, Phishing, and Spam", Realtimepublishers.com, 2005.

[15] P. Manzano, C. Rossow, "Provider Security Measures - Survey on Security and Anti-Spam Measures of Electronic Communication Service Providers", European Network and Information Security Agency, Technical Department, Section Security Policies; Crete, Greece; September 2007.

[16] 2010 Annual Security Report, MessageLabs Intelligence, available at: http://www.messagelabs.com/download.get?filename=MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf (accessed January 2011).

[17] European Union Spam Law: Electronic Communications Privacy Directive 2002. (Directive 2002/58/EC).

[18] Zakon o telekomunikacijama (Narodne novine br. 122/2003).

[19] "Global spam e-mail drops after hacker arrests", BBC News Technology, available at: www.bbc.co.uk/news/technology-11757347 (accessed on December 2010).

[20] Web site with conference data, available at: www.hdmi.hr/mi2009/

[21] Spam Collector, Web site for testing purposes with email listed, available at: www.mefos.hr/dkts

[22] G. Bubaš, T. Orehovački, M. Konecki, "Factors and Predictors of Online Security and Privacy Behaviour", JIOS, vol32.no2, 2008.

[23] S. Gerić, Ž. Hutinski, "Information System Security Threats Classifications", JIOS, Vol31, no.1, 2007.