

AMOUNT OF SPAM IN GLOBAL FREE E-MAIL SERVICES - SIMULATION

Krešimir Šolić, Vesna Ilakovac, Dario Galić

Original scientific paper

Usage of global free e-mail services instead of institutional or company's e-mail addresses can more often cause security drawbacks. Regarding their weaknesses it can be assumed that there will be more unwanted e-mails when using those addresses. In order to receive unwanted e-mail and compare the amount that user receives at different e-mail addresses the authors simulated part of e-mail usage, the one when user registers on different Internet services. Results have shown that the users of the global free e-mail services on average receive significantly more unwanted e-mail compared to the users that use institutional or company's e-mail address. There was also significant difference found among free global e-mail services. Simulation has also shown increasing trend in amount of unwanted e-mail received per month. Regarding these results and previous studies the authors' advice is to prefer institutional or company's e-mail address over free global e-mail services for Internet communication, especially when it is used for professional e-mail communication.

Keywords: e-mail, free e-mail services, security, spam, unwanted mail

Količina spama u svjetskim besplatnim servisima e-pošte - simulacija

Izvorni znanstveni članak

Općenito besplatni svjetski servisi elektroničke pošte su lošijih sigurnosnih karakteristika u usporedbi s adresama elektroničke pošte institucije ili poslovne organizacije. Zbog toga je za očekivati kako će korisnik primati znatno više neželjene elektroničke pošte prilikom korištenja besplatnih svjetskih servisa elektroničke pošte. Kako bi primali neželjenu elektroničku poštu te usporedili količinu koju prima korisnik koristeći besplatnu odnosno institucijsku adresu, autori su simulirali dio komunikacije elektroničkom poštom koji se odnosi na registriranje na razne Internet servise. Iz rezultata simulacije čini se kako korisnici besplatnih svjetski poznatih servisa elektroničke pošte u prosjeku primaju značajno više neželjene elektroničke pošte. Simulacija je također pokazala značajnu razliku između samih besplatnih svjetskih servisa elektroničke pošte te očekivani porast količine neželjene elektroničke pošte s vremenom. S obzirom na rezultate simulacije te prijašnja istraživanja autori preporučuju korisnicima komunikacijskog sustava elektroničke pošte da za komunikaciju daju prednost institucijskim i korporativnim adresama, a pogotovo kad ih koriste za profesionalnu elektroničku komunikaciju.

Ključne riječi: besplatni servisi elektroničke pošte, elektronička pošta, neželjena elektronička pošta, sigurnost, spam

1 Introduction

Important data can be compromised when world-wide popular free e-mail services are used for professional communication through Internet. There are weaknesses regarding e-mail communication system itself [1-3], but generally usage of global e-mail services instead of institutional or company's e-mail addresses can more often cause security drawbacks [4].

There are several reasons that point out possible security weaknesses of those systems compared to institutional or company's ones:

- Previous studies found some weaknesses regarding access through web browser (session hijacking test) [4, 5];
- These services are known around the world and therefore can be of more interest to different sort of hackers [6, 7];
- All data regarding e-mail (and e-mail text itself) is physically in hands of unknown personnel while institutions and companies have some kind of ICT department or employee(s) taking care of e-mail server, accounts, backups and other issues regarding e-mail system (even when outsourced, personal contact is established);
- Because they are free of charge and there is no control when registering for new account false identity is possible by opening e-mail address under somebody else's name if that particular account name at that particular e-mail service is not yet used. In institution or business organization every employee

and only that particular person can get e-mail address under its full name;

- Some of those services forward users' data to third parties. There are personal examples of that and it is also stated in the user's agreement, which is rarely carefully read when registering for new account;
- And also it does not look professional enough to use free instead of institutional or company's e-mail address.

Regarding these weaknesses it can be assumed that there will be more unwanted e-mail (known as spam) when using global and free e-mail services instead of institutional or company's e-mail address. More unwanted e-mail means more viruses, Trojan Horses, worms, spywares and phishing which causes higher possibility for PC infection or user's exploitation.

There is an increasing trend in the amount of unwanted e-mail in overall e-mail traffic and nowadays it has almost reached 90 % of overall traffic [8]. Unwanted e-mail that reaches user's inbox is therefore raising a security problem.

2 Simulation test (tools and methods)

In order to receive unwanted e-mail and compare the amount that user receives in free global vice institutional or company's e-mail addresses the authors simulated part of e-mail communication. E-mail system's usage where user registers on different Internet services (e.g. forums, investment funds, social networks, dating services, etc.) is expected to cause receiving a lot of spam. In a previous

study the authors have proven that this is a productive way to receive a relatively high amount of spam [9].

For simulation purposes the authors opened 7 e-mail addresses in .com domain, as follows: Gmail, Yahoo, Hotmail, AOL, Ommail, Mail2World and Mail. Those addresses were chosen among the most popular global free e-mail services [10]. And there were 8 e-mail addresses in .hr domain opened, the ones that were accessible to authors in different institutions and companies.

On average every second week for a period of one year every one of these 15 e-mail addresses was used in the same way and on the same day. Every e-mail address was accessed by the same web browser, from the same PC and the same Internet connection that day. In this way every e-mail address used in this simulation was equally managed in order to minimize possible influence on the result, the amount of spam received.

After registration to one particular Internet service with every one of 15 used e-mail addresses, authors would activate that service and use it at least once, in order to be certain that that particular Internet service is active and connected to particular e-mail address (and can cause spam). Those Internet services were different forums, investment funds, social networks (e.g. facebook and twitter), dating services, online shopping services, et cetera.

At the end of the simulation period the authors counted the amount of unwanted e-mail received at each e-mail address. Some small amounts of e-mails were excluded, because those were e-mails sent from used e-mail service itself (e.g. self commercials and different system administrator's suggestions).

For comparison of two samples nonparametric statistical test the Mann-Whitney U Test was used and for comparison of absolute frequencies among different free global e-mail services the Chi-square Test was used. Statistical analyses were conducted using the SAS software (version 8.02; SAS Institute INC., Cary, NC, USA) with significance level set at $p < 0,05$.

3 Results

From total amount of unwanted e-mails received, there was on average (mean, e-mail per address) three times more unwanted e-mail received at free global e-mail addresses, than at institutional or company's e-mail addresses (Tab.1). That means significantly less unwanted e-mail received at the second type of e-mail addresses ($p = 0,037$, Mann-Whitney U Test).

Table 1 The amount of spam received during simulation period regarding different type of e-mail address

Type of e-mail address	Total amount of spam/No / %	Amount of spam on average/mean
Global and free e-mail address	181 (72,4)	25,9
Institutional or company's e-mail address	69 (27,6)	8,6
Total	250	16,7
$p = 0,037$, Mann-Whitney U Test		

There was also a significant difference between tested free global e-mail services ($p < 0,001$, Chi-square Test). More than half of unwanted e-mail was received together on Yahoo and Gmail addresses, while the least unwanted e-mail was received on Mail (1 %) address (Tab. 2).

Table 2 Comparison of amount of spam received during simulation period between free global e-mail services

E-mail service	Amount of spam per address/ No(%)
Gmail	46 (25,4)
Yahoo	56 (30,9)
Hotmail	31 (17,1)
AOL	15 (8,3)
Ommail	10 (5,5)
Mail2World	21 (11,6)
Mail	2 (1,2)
Total	181
$p < 0,037$, Chi-square Test	

Possible additional drawbacks for e-mail users that authors got as additional results of the simulation are as follows:

- Spam filter sometimes sorts regular mail into spam folder (e.g. e-mail with activation information);
- User of free e-mail service is obligated to receive periodic commercials of that e-mail provider (as regular e-mail into inbox or as pop-up window), except in case of Ommail service;
- Some of the connections to free e-mail services were relatively slower compared to other free and specially institutional or company's e-mail servers;
- Some free e-mail services had additional drawbacks (e.g. on Hotmail user can send one mail to not more than 10 addresses at once; on Ommail service user has to login at least every three months in order to keep it active...).

Distribution of unwanted e-mail received per month shows expected rising trend, but also inconsistency in that trend (Tab. 3).

Table 3 Distribution of amount of spam received per month

Month	Amount of spam for free services/No	Amount of spam for institutions/No	Amount of spam in total/No / %
March	2	2	4 (1,6)
April	2	1	3 (1,2)
May	0	1	1 (0,4)
June	0	0	0
July	1	1	2 (0,8)
August	1	2	3 (1,2)
September	1	0	1 (0,4)
October	1	0	1 (0,4)
November	17	4	21 (8,4)
December	44	7	51 (20,4)
January	90	37	127 (50,8)
February	23	14	36 (14,4)
Total	181	69	250

Amount of unwanted e-mail per month is unexpectedly low for the last month of simulation period, but complies with previous case study [4]. Also it can be expected that there will be ever more and more spam received per e-mail address in the future simulation period.

4 Conclusion

It seems that users of the global e-mail services on average receive significantly more unwanted e-mail (unwanted commercials, viruses, Trojan Horses, worms, phishing). Because of this and other previously listed drawbacks the authors' attitude is that those e-mail services have a lower security level than the institutional or companies' e-mail addresses.

Therefore the authors' advice is to prefer the institutional or company's e-mail address over free global e-mail services for Internet communication, especially for professional e-mail correspondence. Generally e-mail users are more or less aware of it, but it significantly depends on their technical background knowledge [11].

If free global e-mail services are used they should be handled with precaution and only for personal or occasional usage (e.g. registration on new Internet services). As simulation showed there is also significant difference among different free global e-mail services and users can take that information also in consideration when using these services.

Simulation showed expected increasing trend in the amount of unwanted e-mail received per month, but earlier research showed that with careful usage of e-mail system this trend can be significantly slower [9]. Recommendations for secure usage of e-mail system exists [1, 2, 4] and among them the authors highlight "three e-mail address models": first e-mail address is for professional usage (institutional or company's one), the second one is for private communication (depends on possibilities) and the third one is for occasional usage (free global e-mail address).

One possible limitation of this study is small sample per e-mail type (number of e-mail addresses compared), but results of this simulation can be a starting point for the future research on security issues regarding e-mail communication as part of the ICT system.

5 References

- [1] The 25 Most Common Mistakes in Email Security. // ITSecurity. The Web version (2007), URL: <http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/> (02.11.2011.).
- [2] Top 5 Ways to protect your Email. // ITSecurity. The Web version (2007), URL: <http://www.itsecurity.com/whitepaper/five-essential-steps-to-safer-email-ironport/index.php> (02.11.2011.).
- [3] Min-Hua Shao; Guilin Wang; Jianying Zhou. Some common attacks against certified email protocols and the countermeasures // Computer Communications, 29(2006), pp. 2759-2769.
- [4] Solic, K.; Grgic, K.; Galic, D. A Comparative Study of the Security Level among Different Kind of E-mail Services – Pilot Study // Tehnicki vjesnik-Technical Gazette. 4, 17(2010), pp. 489-492.
- [5] Noiunkar, P.; Chomsiri, T. Top 10 Free Web-Mail Security Test Using Session Hijacking. // IEEE CS ICCIT '08 / P.P. Wang, S. Sohn, G. Dhillon, J. Lee, F.I.S. Ko, N.T. Nuyen, J. Bi, K. Sakurai, et al. 2(2008), pp. 486-490.
- [6] Arrington, M. Gmail Disaster: Reports of Mass Email Deletions. // TechCrunch. The Web version (2006), URL: <http://www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/> (02.11.2011.).
- [7] Stewart, J. Private Email Accounts Go Public Watch. // DeathByEmail. The Web version (2007), URL: <http://www.deathbyemail.com/2007/08/private-email-a.html> (02.11.2011.).
- [8] 2010 Annual Security Report // MessageLabs Intelligence. 2010. URL: http://www.messagelabs.com/download.get?filename=MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf (02.11.2011.).
- [9] Solic, K.; Sebo, D.; Jovic, F.; Ilakovac, V. Possible Decrease of Spam in the Email Communication // IEEE MIPRO / D. Ciscic, Z. Hutinski, M. Baranovic, M. Mauher, L. Ordanic, 2011, pp. 170-173.
- [10] Top 16 Free E-mail Services. // About.com. The Web version (2010), URL: http://email.about.com/od/freeemailreviews/tp/free_email.htm (02.11.2011.).
- [11] Solic, K.; Grgic, K.; Ilakovac, V.; Zagar, D. Usage of the insecure E-mail services among researchers with different scientific background // Medicinski glasnik Ljekarske komore Zenicko-Doboj kantona. 8, 2(2011), pp. 273-276.

Authors' addresses

Krešimir Šolić, dipl. ing.

J. J. Strossmayer University of Osijek,
Faculty of Medicine
Department of Biophysics
Medical Statistics and Medical Informatics
Josipa Huttlera 4, HR-31000 Osijek, Croatia
kresimir@mefos.hr

Prof. dr. sc. Vesna Ilakovac, prof.

J. J. Strossmayer University of Osijek,
Faculty of Medicine
Department of Biophysics
Medical Statistics and Medical Informatics
Josipa Huttlera 4, HR-31000 Osijek, Croatia
vilakov@mefos.hr

Dr. sc. Dario Galic, prof.

J. J. Strossmayer University of Osijek
Faculty of Medicine
Department of Biophysics
Medical Statistics and Medical Informatics
Josipa Huttlera 4, HR-31000 Osijek, Croatia
galic@mefos.hr