Is the spammer evil?

Eleftherios Loukis  
University of Piraeus, Department of Informatics,  
Karaoli & Dimitriou 80, 18534 Piraeus – Greece  
0030 210 4142037  
lbst@unipi.gr

Ioannis Papadakis  
Ionian University, Department of Archives and Library Sciences,  
Ioannou Theotoki 72, 49100 Corfu – Greece  
0030 26610 87408  
papadakis@ionio.gr

Abstract  
The email system has evolved from a great way to communicate, share information and collaborate to 
an inconvenient tool that progressively looses its reliability and becomes obsolete. This paper defines 
the problem, describes its magnitude and discusses the various measures that have been taken so far to 
overcome it. Moreover, it argues that the vast majority of spam could be avoided if so-called spammers 
are confronted as a community of email users with specific, legitimate motives instead of a minority of 
unethical outlaws.

Keywords: email, spam, CAN-SPAM Act

INTRODUCTION

Internet today is a true information highway. Many aspects of the everyday life (social, cultural, 
financial, etc) depend on it in various ways. Its abundant capacity, its global reach and its “no 
gatekeeper” infrastructure are among the most significant reasons why Internet has become an integral 
part of our lives.

However, it seems that the email system, one of Internet’s most widely appreciated applications, has 
followed a rather opposite course. What started out as a great way to communicate, to share 
information, to collaborate, is turning into an inconvenient tool that is progressively loosing its 
reliability and becoming obsolete.

Due to the seriousness of the situation, the Internet society was eventually forced to provide formal 
definitions to the apparent email problem. In this direction, the term ‘spam’ was introduced. 
Surprisingly enough, it has been proven to be very difficult to come up with a definition capable of 
unambiguously identifying all of the emails that are responsible for the email problem. Consequently, a 
widely agreed and working spam definition does not seem to exist.

Beyond the controversy of the term ‘spam’ the email problem is an undisputable reality that needs to 
be confronted. Based on the previously mentioned formal definitions, a number of antispam approaches 
emerged. Such approaches derive from a vast number of disciplines such as law, mathematics, 
statistics, sociology etc. Despite their diversity, they share the common objective of eliminating the 
email problem. Depending on their point of view, current antispam approaches could be classified 
according to the specific goals they are trying to achieve.

In this paper, it is argued that effective antispam solutions should take a closer look at the so-called 
‘spammers’ community, which is comprised of stakeholders with specific motives for relentlessly 
sending countless emails to unsuspected recipients. However, such motives are not necessarily 
unethical. Thus, the members of this community could be classified into three broad classes, depending 
on the various roles an email sender could be associated with. Thus, a sender could be a merchant 
aiming at finding potential customers for his/her products. In this case, there are commercial motives
for sending such emails. In another case, an email sender could be a person wishing to promote his/hers image or ideas to the public (candidate for elections, celebrity, non-profit organizations, etc). In this case, there are promotional motives for sending such emails. Also, email senders could be ill motivated individuals aiming at deceiving their recipients (e.g. spoofing, phishing, chain emails, etc). In this case, there are unethical motives for sending such emails. Maybe, if email senders belonging to the spammers community had the chance to more efficiently direct their emails to the appropriate recipients, their motives would be satisfied and at the same time the email problem would shrink. It should be noted that the above argument does not refer to senders with deceptive motives such as hackers, frauders, etc.

The rest of this paper is structured as follows: Initially, a definition of the email problem is provided. The next section deals with the term spam as a synonym to the email problem. Various existing antispam approaches are mentioned and accordingly classified in the following section. Next, in order to better understand the problem, an effort is made to take into consideration the spammer’s perspective of spam. Finally, conclusions are drawn and the line of thoughts expressed throughout this paper is summarized.

DEFINING THE PROBLEM

Today, the answer to the question “what is your opinion about the email system?” is disappointingly negative as expressed from the vast majority of the Internet society. Alternative forms of Internet communications have emerged (i.e. instant messengers, web 2.0 technologies, social networks etc) that attract the attention of a continuously growing number of Internet users (O’Reilly, 2007). After more than 30 years of prosperity, the email system is currently going through a declining course. Email providers waste time, money and resources in order to route an ever-increasing volume of emails to their clients. Most of the times such emails end up in the trash folder\(^1\). At the same time, email users are daily forced to deal with too many useless emails that clutter their inboxes.

It should be noticed though, that not all useless emails are guilty for the email problem. Useless emails originating from the recipient’s social network were, are and always will be present. Useless emails coming from outside a user’s social network are those responsible for the email problem.

They can be divided into two main categories: objectively useless emails and subjectively useless emails. The former refers to malicious emails that are always useless for everybody (i.e. frauds, viruses, phishing etc) and the latter refers to emails that are useless to a specific set of receivers and/or at a specific period of time (i.e. commercial, promotional, advertisements, etc). For example, there are people that would actually find an email about loosing weight useful while at the same time, other people would consider such an email as annoying. Moreover, people that have already dealt with their weight problem would in all likelihood prefer not to receive emails about loosing weight any more. The above statement defines the subjectivity principle for useless emails.

THE TERM “SPAM”

At present, a widely agreed and workable spam definition does not seem to exist (Schryen, 2007a). This is due to the fact that most of current spam definitions are based on various features of spam (i.e. commercial, bulk, unsolicited), that seem to be only partially valid, resulting in vulnerable ‘anti-spam’ legislation and inefficient software tools against it.

More specifically, spam definitions provided both by the US and Europe are mainly directed towards email produced for commercial purposes (Schryen, 2007b), neglecting other aspects of the email problem such as fraud, phishing, promotional, etc.

Moreover, current spam definitions heavily rely on the term ‘bulk’. Bulkiness refers to the aggregation of identical (or near-identical) emails delivered by an email sender. In contrast, the email problem mostly refers to single emails existing within the cluttered inbox of email recipients. Thus, when trying to decide whether an email is bulk or not we actually have to find out whether this email

\(^1\) Spam-o-meter Statistics By Percentage: Spam statistics, Available at: http://www.spam-o-meter.com accessed 15 September 2008
originates from a single sender that has massivly sent identical (or near-identical) emails. Such a task is quite often difficult to accomplish, despite current efforts in collaborative antispam solutions (Ramachandran et al., 2006).

The term ‘unsolicited’ is also commonly met in current spam definitions. However, the fact that spam is unsolicited should not imply that only spam is unsolicited. The very nature of the email process partly relies on unsolicited communication. Thus, useful emails being sent without prior consent from their recipients could be mistakenly considered as spam. Besides, even if a recipient has agreed to receive an email, how and when such consensus is established, may not be obvious. It is very difficult to know whether a relationship between the sender and the recipient already exists or not. To make things worse, even if such a relationship does not exist, there is a lot to be done before accusing the sender for improperly harvesting the recipient’s email address. Ultimately, engaging the term ‘unsolicited’ in the context of spam definition seems to lead to more problems than solutions, at least as far as legislation is concerned.

It should also be taken under consideration that emails which are considered as part of the email problem from 90% of their recipients, are considered as useful from the remaining 10%. Engaging subjectivity within a formal definition renders such definition as erroneous.

Spam could be correctly associated with the act of repeatedly sending the same email to specific recipients. However, spam has evolved in a way that exactly the same email seldom finds its way to the same inbox. Senders usually make minor changes to an email before sending it to receivers that have already received a similar one. Thus, definitions containing such a term could be considered as controversial.

Two more terms finding their way into many spam definitions (Schryen, 2007a) are ‘untargeted’ and ‘indiscriminate’. Similarly to the arguments about ‘unsolicited’, these two terms characterize many emails that are not necessarily considered as spam. Moreover, it is difficult to prove whether an email was indiscriminately sent from its sender.

Quite often, emails that are considered as part of the email problem have certain properties (i.e. anonymous and/or disguised emails with deceptive, fraudulent, illegal or offensive content). However, it is risky for formal definitions of spam to incorporate such properties. Not all emails considered as spam have such properties. Thus, even just one spam email that does not have any of the above properties is enough to cause problems both to legislative approaches and antispam mechanisms.

Moreover, the fact that formal definitions of spam do not take under consideration the previously mentioned subjectivity principle for useless emails, renders such definitions as cumbersome: an email has to be treated as spam for all occasions, at all times for everybody.

Beyond the controversy of the term ‘spam’ the email problem is an undisputable reality that needs to be solved. Based on the previously mentioned formal definitions, a number of antispam approaches have been proposed. However, it seems that in the name of the crusade against spam, some approaches unintentionally contribute to the overall email decline. For example, when useful emails are mistakenly filtered as spam and thus never make it to the recipients’ inbox, unreliability is added as another drawback to the already suffering email system.

ANTISPAM APPROACHES

Given the fact that the email problem is apparent to everyone, it is necessary to take a closer look at current antispam approaches in order to track down their vulnerabilities. By doing so, we will be able to avoid pitfalls and propose truly viable solutions that will eliminate, or at least reduce the overall email problem.

In order to better understand current trends in fighting against spam, antispam approaches should be classified into a consistent taxonomy. However, by taking a closer look at the corresponding literature, it appears that it is not an easy task to create such taxonomy. Indeed, many antispam efforts seem to have ambiguous origin, thus being eligible to be classified in more than one category.

Conversely, many existing taxonomies consist of categories with vaguely defined borders, thus allowing such categories to host more than one approach simultaneously. For example, in (Judge, 2006) the category labeled as “legal prosecution” is a subclass of “spam responses” whereas it could
easily be a member of “spam deterrence approaches”, since “legal prosecution” is a discouraging factor for anybody thinking of sending junk email.

Having the above thoughts in mind, a simple taxonomy is proposed aiming at unambiguously classifying current antispam approaches into two mutually exclusive categories: The first category contains approaches aiming at preventing the act of spam. Usually, prevention is accomplished by discouraging potential spammers. The second category contains approaches that can only be put into action after the birth of spam. Spam is being born at the time when a spammer actually sends emails. In their majority, the main objective of approaches belonging to this category is to hide the problem from the users instead of solving it: despite the fact that spam never arrives to end users, ISPs suffer from resource abuse due to the amount of spam reaching their servers. Thus, the consequences of spam indirectly reflect to end users (i.e. delays, denial of service, etc).

From another point of view, the proposed taxonomy consists of one category aiming at confronting the true causes of spam (i.e. ‘Prevention’) and another one focusing on eliminating the consequences of spam (i.e. ‘Suppression’).

![Figure 1. Proposed antispam approaches taxonomy](image)

As illustrated in figure 1, there are two main categories for spam prevention, namely “email authentication” and “law”. On the other hand, “policy enforcement”, “filtering”, “network – clue analyzing” and “behavioral” belong to the spam suppression category. A detailed description of these approaches is presented in the following section.

**Email authentication techniques**

The lack of authentication is perhaps the most significant vulnerability of the email system. A functional authentication system, incorporated within a framework capable of punishing the ones responsible for today’s email problem (spammers, phishers, virus creators, etc), in all likelihood deter malicious email users from sending junk emails.

However, it seems that incorporating authentication in the email system is far from a trivial procedure due to two important reasons: First of all, Internet users are accustomed to a mostly anonymous environment that exercises no control over their actions. Thus, any kind of authentication could be faced with reluctance and distrust, since users would have to comply with additional constraints. In addition, the act of authentication is by itself an additional burden for users that have to be convinced for its necessity. Secondly, email vendors would also be reluctant in deploying email authentication systems. Such deployments usually require fundamental changes to existing email infrastructures (e.g. policies (Lawton, 2006)) for which a great deal of resources have already been invested in terms of money, time and expertise.

To make things worse, even if email authentication was considered as well-established, the email problem could get worse due to the existence of computers that have remotely been taken under the
control of spammers, thus operating as “zombies”. Indeed, within such an environment, it would be difficult to prove that the authenticated sender of an email identified as spam is not the one that actually sent it. As a result, innocent, technologically naive users would be mistakenly accused as spammers just because their computers have been operating as zombies (Levy, 2003).

Law

In terms of legality, most countries and regimes that provide legal frameworks against spam are influenced by the rationale of the opt-in or opt-out approaches (Moustakas et al., 2005). In an opt-in system, unsolicited communications – in this case emails sent to recipients without their prior consent – are considered illegal. In an opt-out system, the sender is allowed to send the first email to each recipient, provided that it contains an option to allow the receiver to declare that he/she doesn’t wish to get any additional emails from the sender. Whether spam is legal or not depends upon the opt-in or opt-out choice exercised by the recipient of the communications and also on the legal system of reference (Lugaresi, 2004).

It could be argued that the opt-out approach justifies the action of sending spam at least for the first time. From another point of view, in an opt-in solution a spam is prohibited before the spammer has a chance to communicate it, thus eventually restricting freedom of speech (Fingerman, 2004).

European Union’s – EU’s approach against spam mostly focuses on protecting consumers’ privacy and economic interests. Specifically, EU laws and directives do not clearly define the term “spam” and the enforcement of an implied opt-out approach is restricted to natural persons only. Based on these principles, EU solution should not be regarded as the ultimate answer to spam, but as an attempt to provide for its Member States a rational discipline together with a possible model for a harmonized approach to reducing spam (Lugaresi, 2004).

On the other hand, the United States’ Congress enforced the CAN-SPAM Act, which also envisions fighting spam in legal terms. It is primarily targeted towards unsolicited commercial “spam” email, which is punished by imposing stiff civil penalties and even prison sentences to parties convicted of spamming (Leavitt, 2007). The CAN-SPAM Act is based on the opt-out model. Unfortunately, according to surveys (Soma et al., 2008), the CAN-SPAM Act has had little consequence since going into effect on January 2004. One major drawback of the CAN-SPAM Act is that it drives spammers to hire short-term employees or form shell corporations or otherwise come up with temporary accounts under which to send spam. Moreover, it fails to take under consideration the knowledge of other countries that have tested opt-out legislation and have discovered that it simply does not work (Soma et al., 2008). It is also disappointing that the CAN-SPAM Act is working towards comprehensive “do not email” lists. Indeed, such lists may be dangerous for users’ privacy. Apart from security concerns, the risk is to end up with a Big Brother effect (Lugaresi, 2004).

A broader argument against legislation-based solutions to the spam problem (including the US and Europe) is that such legislations are only enforceable within the corresponding regime. Thus, spammers change their tactics or simply move their servers to locations without antispam regulations (Moustakas et al., 2005). Consequently, Internet’s universality renders the enforcement of a global antispam legislation as a very difficult task to achieve.

Finally, defining yet another problematic antispam law may lead to the opposite effect of legitimizing gigantic amounts of spam (Goodman et al., 2007).

Policy enforcement (Pricing - Hips - Delay)

Policy enforcement is based on reducing the effortlessness of sending email, by changing the action of sending email. This can be achieved either by pricing emails, or by requiring senders to solve some kind of puzzle (Human Interactive Problem Solving - hips (von Ahn et al., 2003)) or by simply

---

2 Article 1, Dir. 2000/31/EC, accessed Apr. 7, 2008
consuming additional resources from the email sender (e.g. the Penny Black Project\textsuperscript{4} and others ([Cobb, 2008], [Dwork et al., 1993], [Loder et al., 2004]).

Such techniques may be applied in an ‘as-is’ basis (Hansel, 2004), where all email senders are burdened for each message they send. Alternatively, they could be integrated with spammer identification systems where additional burden is only applied to potential spammers. Consequently, spammers have to think twice before sending spam messages due to the considerable effort required for the sending action.

However, many of the above methods depend on authentication infrastructures that are currently not widely available to the Internet society. Moreover, the additional transactions required for sending email (e.g. challenge-response systems), affect the overall Internet’s performance.

And finally, from a social point of view, email users will most likely find the additional burden cumbersome, e.g. by repeatedly being asked to solve a puzzle or being charged for each email they send.

Filtering

This category refers to antispam approaches relying on various kinds of filters in order to decide which email should be considered as spam. Filtering is maybe the most popular method for fighting spam.

There are several kinds of filters available. Depending on the approach method, such filters may be divided into several classes: Thus, one could come across a) individual and collaborative filters (Gray et al., 2004), b) statistical content-based filters, c) static and learning ones, and d) standalone/server-side filters (Garcia et al., 2004).

However, despite the considerable popularity of such approaches, there are a number of issues that inevitably come under discussion.

Initially, the inherent possibility of mistakenly classifying legitimate emails as spam (i.e. false positives) is one of the most serious drawbacks of antispam filtering (Graham, 2004). According to (Yih et al., 2006), users’ criteria in selecting antispam filters are not based on their success on blocking as much spam as possible. Instead, they prefer filters that feature low rate of false positives. No matter how sophisticated a filter is, there is always the possibility of blocking legitimate email as spam. Moreover, the evolution of spam techniques over time, leads to the conclusion that spammers are practically unpredictable. Currently, there are spam techniques that manage to bypass filters by employing various methods (images instead of text, poems, obfuscation, etc (Yerazunis, 2004), (Hulten et al., 2004)). It seems realistic to claim that any weaknesses of current or future spam filters will eventually be exploited by spammers (Lowd et al., 2004).

Last but not least, common spam filtering applications eventually hide the spam problem from users instead of eliminating it. They classify and/or delete spam messages after they’ve been received by systems, but by then much of the bandwidth and processing costs of the spam have already been wasted (Goodman et al., 2007).

To sum up, despite the wide propagation of various filtering models, it seems that the false positives phenomenon will always be a discouraging factor of adopting this kind of antispam approach.

Network - Clue Analyzing

This category contains approaches trying to identify either spam messages or spam servers by monitoring the trails that are being left by the action of sending an email in order to detect suspicious elements.

Approaches belonging to this class focus on examining the context of an email (e.g. recipient’s email account, IP address, etc), in contrast to the previous class (i.e. filtering) which contains approaches trying to identify spam messages from their main content. Apart from this difference, both categories aim at identifying spam emails by processing emails that have been arrived at the receiver’s ISP.

Consequently, this category has many of the drawbacks mentioned in the previous section, such as false positives, false negatives, wasting of resources, etc.

**Behavioral**

Behavioral approaches are trying to fight spam by maintaining registries of already known spam messages and/or spam machines. Such registries are commonly known as lists (e.g. SORBS\(^5\), Spamhaus\(^6\), SpamCop\(^7\), SURBLs\(^8\), etc). They may be managed either locally by individual users through appropriately designed email clients or published online in so-called collaborative lists. This category comes as a complement to previous categories since messages should already have been created, sent and identified as spam.

However, similarly to the previously mentioned classes “clue analyzing” and “filtering”, behavioral approaches are targeted towards the symptoms of the problem (i.e. end-user annoyance) instead of the actual causes. Such approaches not only aim in hiding the consequences of spam from end-users but also they take no measures at all to relieve other parties involved in the email life-cycle (e.g. ISPs). Moreover, the above approaches implicitly raise the issue of correctly identifying the entity to punish. Thus, in the case of a company (i.e. stakeholder) delegating a spammer to send commercial unsolicited bulk emails through a possibly unaware ISP or a compromised machine (i.e. zombie), the question “who should eventually take the blame?” arises. Possible answers include the stakeholder, the spammer, the ISP and the ignorant user of a compromised machine. Finally, blocking spam through the employment of various kinds of blacklists is prone to the fact that there might be a considerable time lag between the creation of a new spam entity and its discovery/inclusion in a list (Pu et al., 2004). Thus, the spammer may already have achieved the anticipated goals and the receiver may already have suffered the corresponding consequences.

**Hybrid**

Apart from the aforementioned classes for fighting spam, there are also some efforts that try to integrate a number of individual strategies into a single system. Obviously, such hybrid solutions inherit not only the benefits but also the drawbacks of the integrated subsystems. Consequently, their main effort is to compensate the drawbacks of one contained approach with the advantages of another. Ideally, the final system results in an all-in-one robust antispam approach, which performs better as a unified whole than the aggregation of its subparts.

For example, spamassassin\(^9\) is based on content-matching rules, also supporting DNS-based, checksum-based and statistical filtering, powered by external programs and online collaboration lists. It is considered as a promising solution to the email problem, even though, as stated earlier, it has to deal with a number of issues accumulated from the techniques it encompasses.

**DECONSTRUCTING SPAMMER**

So far, a number of different antispam approaches have been mentioned, based on the common assumption that the spammer is a malicious entity, aiming at circulating large volumes of spam. However, not all spam is useless. Indeed, the previously mentioned subjectivity principle dictates that the same email that has been flagged as “spam” from one recipient could be flagged as “not spam” from another one, or, even from the same recipient at another time. Moreover, the fact that 10% of spam constitutes the starting point of some kind of transaction (Weiss, 2003), renders such emails as potentially useful.

As it is mentioned throughout this paper, there are different definitions, approaches and perspectives concerning the email problem. Yet, everybody agrees to one common thing: too much useless email is circulated. So-called “spammers” abuse the email system by sending enormous amounts of email.

---

7 SpamCop, [www.spamcop.net](http://www.spamcop.net), accessed Sept. 1, 2008
Consequently, in order to find out the reasons of the email problem, it should be investigated why the email system is abused.

First of all, it is reasonable to assume that the email system wouldn’t be abused without significant motives from the ones that abuse it. Such motives could be organized in a number of distinct categories, depending on the various roles an email sender (or an agent acting on his behalf) can be associated to. Thus, a sender could be a merchant aiming at finding potential customers for his/her products. In this case, there are commercial motives for sending such emails. In another case, an email sender could be a person wishing to promote his/her image or ideas to the public (candidate for elections, celebrity, non-profit organizations, etc). In this case, there are promotional motives for sending spam. Also, email senders could be ill motivated individuals aiming at deceiving their recipients (e.g. spoofing, phishing, chain emails, etc). In this case, there are malicious motives for sending such emails. It is the authors’ belief that the above three kinds of motives apply to the vast majority of senders causing the email problem.

Apart from the ill-motivated senders (i.e. hackers, frauders, etc), many of the so-called spammers aim at locating the minority of recipients that will consider their email as useful (e.g. customers, voters). Thus, most spammers have ordinary promotional, and/or commercial motives. However, the existing email infrastructure does not provide a way to properly satisfy such motives without circulating unsolicited emails in bulk rendering the whole system annoying for its users. At the same time, spammers are also unhappy with today’s reality: due to the aforementioned antispam measures, they have to make special efforts to deliver messages (e.g. disguising messages, and/or sending individual email messages rather than batching them together as bulk messages) before sending them to their recipients.

Maybe, if spammers had the chance to more efficiently direct their emails to the appropriate recipients, their goals would be satisfied and at the same time the email problem would be reduced. It should be noted once again that the above argument does not refer to senders with deceptive motives such as hackers, frauders, etc.

TOWARDS A MOTIVE-SENSITIVE EMAIL SYSTEM

As stated earlier in this paper, there are three main categories of motives for sending spam, namely commercial, promotional and malicious. Efficient solutions to the email problem should take into account such motives that practically represent the spammers perspective to the email problem.

Emails deriving from spammers with malicious motives can only be dealt with through appropriate suppression actions (e.g. laws, punishment, etc). On the other hand, it is argued that promotional and/or commercial motives should not be considered as punishable actions, despite the fact that they are greatly responsible for today’s decline of the email system. In this context, it might be possible to satisfy the requirements of spammers with promotional and/or commercial motives without putting additional strain on the email community (i.e. email receivers, ISPs, etc). For example, email senders could be provided with the opportunity to tag the context of their emails according to a well-established taxonomy of email categories (e.g. food, commercial, leisure, etc). At the same time, receivers could be provided with the opportunity to decide a priori what kind of emails to receive. Such decisions could be based on their personal preferences.

Solutions to the email problem should not just focus on fulfilling receivers’ needs that consider spam as useless. It is equally important to take into account the minority of receivers that do not consider such emails as useless. Ultimately, such solutions would result in much less spam originating from a minority of ill-motivated spammers.

Finally, it is argued that most of the identified causes of the email problem exist due to the lack of respect exercised by a minority of people (i.e. email abusers) towards the broader email community. To that effect, proper education concerning Internet ethics could prevent the spreading of such beliefs and provide a solid background for the forthcoming solutions.
CONCLUSIONS

It is common knowledge that a number of serious problems has brought the email system to its knees. Nowadays, the need to act upon such problems is more pressing than ever. Having these thoughts in mind, this paper performs a comprehensive review of the email status.

Specifically, an attempt is made to define the problem, in order to accurately determine the main aspects of this phenomenon. In this context, it seems that the widely used term “spam” is only partially capable of providing a semantic equivalent to the email problem. A classification of current approaches aiming at offering solutions is also provided in an attempt to determine their weak spots, which prevent them from being effective. Further analysis takes under consideration the email abuser’s perspective. Thus, in order to deal with the email problem, it is proposed that modern email systems should find a way to regulate promotional and/or commercial emails while at the same time eliminate malicious ones.

REFERENCES


A. Weiss (June 2003), Ending Spam’s Free Ride, netWorker, 7 (no. 2), 18-24.


D. Fingerman (2004), Spam canned throughout the land?, Summary of the CAN-SPAM Act, Journal of Internet Law, 7 (no. 8), 11-17.

N. Leavitt (March, 2007), Vendors Fight Spam’s Sudden Rise, IEEE Computer, 40 (no. 3), 16–19.


J. Goodman, G.V. Cormack, and D. Heckerman (2007), Spam and the ongoing battle for the inbox, Communications of the ACM, 50 (no. 2), 25–33.


W. Yih, J. Goodman, and G. Hulten (2006), Learning at Low False Positive Rates, in Proc. Second Conf. on Email and Anti-Spam (CEAS 2006), California USA.