

**CLOUDMARK** AUTHORITY

## Applying Predictive Classifiers to Eliminate Email Abuse in the Enterprise

© 2005 Cloudmark, Inc. All rights reserved.  
Published March 2005

Inquiries: [bd@cloudmark.com](mailto:bd@cloudmark.com)

Cloudmark, the Cloudmark logo, Authority, and SpamNet are trademarks or registered trademarks of Cloudmark Inc., for use in the United States and other countries. SPAM (all uppercase) is a registered trademark of Hormel Foods Corp. All other product or service names may be trademarks, registered trademarks, or service marks of their respective owners.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Cloudmark, Inc.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice. Cloudmark shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this publication or examples contained herein.

Cloudmark, Inc.  
128 King Street, 2<sup>nd</sup> Floor  
San Francisco, CA 94107  
Phone: 415-543-1220  
Fax: 415-543-1233  
[www.cloudmark.com](http://www.cloudmark.com)

# Table of Contents

OVERVIEW .....	4
SPAM, SPAM, MORE SPAM, AND NOW PHISHING .....	5
TRADITIONAL TECHNIQUES OF IDENTIFYING EMAIL ABUSE: .....	6
Blacklists and Whitelists .....	6
Rules-based Filters.....	6
Heuristics.....	6
Challenge / Response .....	6
Bonded Sender.....	7
Bayesian Classification.....	7
The Cocktail.....	7
THE CLOUDMARK ADVANCED METHOD.....	8
Predictive Modeling .....	8
Classification .....	8
Real-time Feedback from the Industry’s Most Trusted Community.....	8
Real-time Reputation Data Service Updates.....	9
Zero-time Protection from Email Abuse.....	9
High Accuracy and Low False Positives.....	9
High Message Throughput and Low Resource Utilization.....	9
Improved and Flexible Management .....	9
CONCLUSION .....	10

## Overview

Today's enterprises are faced with increasingly sophisticated forms of email abuse, which threaten the viability of email as a corporate communication tool. Enterprises require a solution that delivers real-time anti-spam and anti-phishing protection to address the limited time window in which these attacks occur.

This paper explains why traditional anti-spam technologies are not equipped to deal with the scope and severity of today's attacks and proposes a superior method of combating email abuse. Cloudmark's award-winning technology fights spam, phishing and other forms of email abuse with a proven 98+% accuracy rate and near-zero false positives<sup>1</sup>. Unlike other vendors, Cloudmark solutions automatically adapt in real time to new threats.

Leveraging feedback from the Cloudmark trusted and collaborative community of over 1 million users, Cloudmark delivers the first and only solution that applies real-time reputation data updates and powerful predictive algorithms to effectively eradicate email abuse in enterprises today.

---

<sup>1</sup> PC Magazine Editor's Choice 04 and Best Performance two years in a row (Feb 04 and Nov 03)

## Spam, Spam, More Spam, and Now Phishing

The number, complexity, and speed of attacks are rising along with the costs to enterprises. More recently, spam has become the vector for spyware and worm infection. Its adult content creates a hostile work environment and its cost as well as impact should not be underestimated.

Phishing attacks which lure unsuspecting recipients to type passwords, credit card details, or other sensitive information into fake web sites increased threefold during the first half of 2004. Phishing attacks are now targeting enterprises by compromising ISP and extranet account information.

The worldwide estimated cost of spam and phishing attacks in 2005 is \$50 billion<sup>2</sup>, and includes:

- Lost productivity as workers sort, delete, read, and click through spam messages.
- Need for more servers, network infrastructure, and IT employees to deal with the skyrocketing volume of email.
- Legal exposure as employees offended by sexually explicit spam seek recourse.
- Risk of corporate data being compromised through phishing attacks exposing employee identities.

---

<sup>2</sup> Ferris Research, Webinar Presentation, Spam Costs: Global Economic Impact in 2005, March 2005

## Traditional Techniques of Identifying Email Abuse: Why They Fail

Over the years, a long roster of techniques for eradicating spam has evolved. Some have changed little since their inception, merely ballooning in size as they struggle to stay one step behind spam's constantly evolving nature.

### Blacklists and Whitelists

Blacklists attempt to identify suspected spammers or suspected email sources, keeping their messages out. Whitelists identify legitimate sources of email and ensure delivery.

Unfortunately, blacklists and whitelists are beset with problems. They can be fooled by both spoofing (relaying of email through a chain of unsuspecting servers) and by zombie attacks (legitimate user machines hacked to originate email on the user's behalf).

Blacklists and whitelists also require maintenance, either manually by end users or by administrators. Given the sophistication of today's attacks, such static maintenance is prone to gross error, since white or blacklisted reputations can change in hours.

### Rules-based Filters

Rules-based filters are a reactionary approach. Filtering rules, which are based on content, cannot be used in isolation because of their ineffectiveness.

Tens of thousands of rules are required to keep pace. New spam can be blocked only after an initial specimen is obtained and analyzed. By the time a new rule is written and deployed, the message may have changed, rendering the rule useless. Rules are also language specific and need to be developed on a per language and spam-variant basis.

Rules-based filters require constant updating placing a huge strain on IT departments, network infrastructure, and providing a pathway to hackers from the outside world.

### Heuristics

As an extension of rules-based filtering, heuristics shares the same chief shortcoming: the database of rules grows endlessly. Heuristic solutions analyze large quantities of spam and identify trends. Based on aggregated results, each message is given a score. If the score meets or exceeds a preset value, the message is classified as spam.

Heuristic analysis falls short. It is a linear process that cannot easily adapt to the ever-changing characteristics of spam, leading to inevitable collateral damage as legitimate messages are blocked.

### Challenge / Response

The basis of most challenge/response (CR) tests is that email from an unknown sender initially is rejected, but after that sender passes a one-time test, mail is delivered. For the network, storage requirements increase as messages waiting for the response to the test question are held.

The major drawback of CR is that spammers know that the domain is protected. Asking the challenge question alerts the spammer that the recipient's address is valid.

CR may quadruple email traffic. For an unknown sender, four messages, instead of one are required: receive the original message, send the challenge, receive the response, and notify the sender of the pass-or-fail result.

## Bonded Sender

Promise that your company won't send spam, back up that promise with a financial pledge, and you could be designated a bonded or warranted sender. This is not an anti-spam solution, merely a cash-backed pledge to behave. Break your word, and you'll be charged a penalty by the bonding company.

Bonding systems are not interoperable, requiring each anti-spam vendor to adapt its products to work with multiple bonding systems. Furthermore, bonding companies have not yet established a record of equitable and efficient judgment.

## Bayesian Classification

Bayesian Classification represents a Machine-Learning System (MLS) rooted in statistical theory and focused on modeling a larger body (all email messages) from a smaller body (emails a user specifically identifies as Legitimate or Spam). Most common implementations of this type of filter rely on the frequency of individual words or phrases within the body of a message as indicators of the overall disposition of the message.

The major constraint of a Bayesian Classifier is that the sample from which it learns (the smaller body of mail a user identifies) must statistically represent the larger body (all email a user or a corporation receives), otherwise the predictions it generates are likely to be incorrect. Realistically, each individual will receive different types of email according to their job function and interests. The end result is a large and varied body of email, which makes it impossible for a Bayesian Classifier to accurately identify spam or otherwise.

## The Cocktail

None of the preceding techniques are comprehensive enough to stand alone in identifying and eradicating spam. Out of necessity, combinations are universally employed. With a bewildering array of combinations and permutations possible, zeroing in on the best one for any particular enterprise is largely a matter of conjecture and trial-and-error.

## The Cloudmark Advanced Method

Cloudmark's gateway enterprise anti-spam solution, Authority, introduces a fully automated process of capturing, analyzing and predicting spam, phishing and other forms of email abuse. Authority employs a sequence of powerful algorithms – the Predictive Classifier, which work in conjunction with real-time updates from the Cloudmark community to block spam, phishing, and additionally, many viruses and spyware. Authority's advanced methods do not require additional network infrastructure or manual intervention, freeing up valuable administrator time.

### Predictive Modeling

Cloudmark research has identified, sequenced, and documented approximately 300 individual algorithms, which form the Predictive Classifier. These algorithms key in on spam attributes of a message (for example, a malformed header), while others identify points of message legitimacy (such as appropriate message encoding). Maintaining fewer than 300 algorithms requires far less effort than maintaining a database containing tens of thousands of filtering rules. Therefore, this model scales exceptionally well for enterprises.

Using mathematical techniques, each incoming message is evaluated by ascertaining its inherent characteristics and mapping them to the sequence of selected algorithms. As the number of mapped characteristics climbs, it becomes possible to predict, with increasing degrees of confidence, whether the message, and others similar to it, are, or will be, spam. For example, even though the subject text in a message may have changed from "Make Money Fast" to "Earn Cash Quickly," and the message's overall appearance altered too, its underlying technical structure has not, a key factor leveraged by Cloudmark Authority. Understand the predictable structure of a message, and the need to create a growing mountain of filtering rules becomes unnecessary.

Cloudmark's emphasis of underlying message structure over the content contained in that message sets it apart from all other spam-fighting products.

### Classification

While other anti-spam solutions may declare a message as either spam or not-spam, Authority's predictive classifier assigns each message a Spam Confidence Level of 0 percent to 100 percent. A message with a 3 percent confidence level almost certainly is legitimate, while one with a 98 percent score is undoubtedly spam. Based on the confidence score, different message-handling policies can be applied, ranging from unimpeded delivery, to quarantine or outright deletion.

### Real-time Feedback from the Industry's Most Trusted Community

Cloudmark has the world's most trusted database of spam, phishing, and other email threats. Reports from 1 million trusted users in 160 countries are corroborated to provide accurate and unspoofable data. It is the size and scope of this database, which fuels the training that

provides the highest accuracy levels in Authority's Predictive Classifier. At Cloudmark this data is used to train new predictive algorithms, which are fed into Anti-spam cartridges and typically released every 30 days.

### Real-time Reputation Data Service Updates

Cloudmark provides Micro Updates on an hourly basis, enabling Authority to stay current with fast-moving phishing attacks. Authority maintains the highest levels of accuracy and near-zero false positives on phishing emails, and as well legitimate financial institution mailing.

### Zero-time Protection from Email Abuse

Cloudmark is able to handle new varieties of email abuse proactively and automatically, rather than reactively and manually. Cloudmark successfully identified the Sobig virus due to its anomalous makeup, and successfully blocked it many hours before anti-virus companies provided virus signature updates.

### High Accuracy and Low False Positives

Cloudmark solutions are consistently amongst the most accurate and provide the lowest false positive of any in the industry. Authority's high accuracy levels can also be attributed to techniques independent of language, encoding, dictionary or phraseology.

### High Message Throughput and Low Resource Utilization

Cloudmark Authority uses an efficiently trained set of under 300 highly optimized algorithms, which uses less CPU and memory resources than other solutions available today. In addition, Cloudmark Authority offers a higher throughput than competing solutions.

Cloudmark Authority can optionally be installed on a corporation's existing 1 message transport agent (MTA), saving thousands of dollars in hardware acquisition costs and perpetual administrative expenses.

Cloudmark Authority exacts a performance overhead of only 5 percent to 10 percent. Other solutions have a performance penalty of up to 40 percent, usually resulting in the need for one or more dedicated servers.

### Improved and Flexible Management

Creating message handling policies and tiers for delivering, detaining, or deleting incoming mail is accomplished through a browser-based interface. Cloudmark requires minimum management.

For email and IT administrators, a variety of statistical reports can be generated and viewed through a browser interface, including percentages of spam and legitimate mail, mail-handling policy analysis, corporate dollars saved, and aggregate employee time saved.

## Conclusion

Authority eradicates spam through its powerful Predictive Classifier and with real-time Micro Updates derived from the Cloudmark trusted community. It is a predictive solution with the power to handle future levels of spam and phishing attacks, and as well other forms of email abuse. Authority has a negligible impact upon mail gateway performance and is a scalable solution, ready to handle high-volume enterprise email streams.

Cloudmark Authority is the solution that can be relied up for high performance and industry-leading accuracy, delivering a cost effective solution for today's enterprises.