

RAV AntiVirus fighting spam

First Release Date: January 14, 2003

Current white paper revision: 1.0

Address: 223, Mihai Bravu Blvd, 3rd district, Bucharest, Romania
Phone/Fax: +40-21-321.78.03, **Hotline:** +40-21-321.78.59

CONTENTS

Why am I getting spam?	3
What is spam?	3
How spammers operate	3
Why is spam so bad, after all?	4
What to do	5
How to limit spam	5
How does RAV AntiVirus fight spam?	6
How does the Antispam work in RAV AntiVirus for Mail Servers?	6
Useful links.....	7

Why am I getting spam?

Is your e-mail address on any Web pages? Do you post to public newsgroups? Did you fill out online forms on dubious sites? Or did you correspond with companies you know nothing about via e-mail? If the answer to any of these questions is "Yes", you are the likely receiver of SPAM.

What is spam?

The term "spam" is refers to **unsolicited commercial e-mail** or **unsolicited bulk e-mail**, i.e. e-mail that you did not request. Most often spam contains advertisements for dubious services or products.

How spammers operate

Unlike junk paper mail, e-mail spam costs the sender very little to send; almost all of the costs are paid by the recipient and the carriers, because the spammer does not have to pay for all the Internet bandwidth tied up in the delivery of the spam. Because they have no incentive to be efficient in their mass e-mailing, spammers usually don't put much effort into verifying e-mail addresses. They use automatic programs called bots to scour the Web and Usenet newsgroups, collecting addresses, or buy them in bulk from other companies.

One of most common tricks used by spammers is to relay messages through the e-mail server of an innocent third party. This tactic doubles the damages: both the receiving system and the innocent relay system are flooded with spam. And for any mail that gets through, often the flood of complaints goes back to the innocent site because it was made to look like the origin of the spam. Many spammers send their spam from a free account from a large ISP such as AOL, Yahoo!, or Hotmail, then abandon the account and open a new one to use for the next assault. Another common trick that spammers use is to forge the headers of messages, making it appear as though the message originated elsewhere. This is called spoofed e-mail. There are some pieces of information in the full headers that the spammer cannot forge, but even after technical investigation into the source of the message, most often the resulting information leads to a dead end.

Common types of spam

The most commonly seen spam includes the following:

- Chain letters
- Pyramid schemes
- Multilevel marketing
- "Make Money Fast" schemes
- Foreign bank scams
- Offers of phone sex lines and ads for pornographic Web sites
- Illegally pirated software

According to a poll conducted and released by Harris Interactive, 80 percent of users say they find spam very annoying, a huge increase from the 49 percent who felt that way two and a half years ago. Strong support for a legal spam ban crosses gender, color, ethnic and political party lines.

While many people are annoyed by many different kinds of spam, messages selling pornography (91%), mortgages and loans (79%), investments (68%) and real estate (61%) annoy the largest number of people. The poll was taken with 2,221 Internet users aged 18 and older, during Nov. 22 - Dec. 2, 2002.

You can find the poll using this link:

<http://www.harrisinteractive.com/>

Why is spam so bad, after all?

- **It's almost free for the spammer to send it.** Spam is unique in that the receiver pays so much more for it than the sender does. For example, AOL has said that they were receiving 1.8 million spams from Cyber Promotions per day until they got a court injunction to stop it. Assuming that it takes the typical AOL user only 10 seconds to identify and discard a message, that's still 5,000 hours per day of connect time per day spent discarding their spam, just on AOL. No other kind of advertising costs the advertiser so little, and the recipient so much.
- **Generates problems.** Many spam messages say "please send a REMOVE message to get off our list." At the moment, most of us only get a few spams per day. But if only one thousandth of the Internet users decided to send out spam at a moderate rate of 100,000 per day (easily achievable with a dial-up account and a PC): everyone would receive 100 spams every day. If spam grows, it will crowd our mailboxes to the point that they're not useful for real mail.
- **Consuming resources.** An increasing number of spammers send most or all of their mail via innocent intermediate systems, to avoid blocks that many systems have placed against mail coming directly from the spammers' systems. Many other spammers use "hit and run" spamming: they get a trial dial-up account at an Internet provider for a few days, send thousands of messages, then abandon the account. The unsuspecting provider has to waste staff time for cleanup and monitoring their trial accounts for abuse.
- **Rubbish, rubbish, rubbish.** The spam messages have almost without exception advertised stuff that's worthless, deceptive, and partly or entirely fraudulent: spam software, funky miracle cures, off-brand computer parts, vaguely described get rich quick schemes, dial-a-porn, and so on.
- **You can get yourself into trouble.** Some kinds of spam are illegal in some countries on the Internet. Especially with pornography, mere possession of such material can be enough to put the recipient in jail.

Did you know that...

- In the workplace, research company Gartner estimates that roughly 25 percent to 35 percent of a company's total mail volume consists of spam.
- Spam is costing \$8.9 billion to U.S. corporations, \$2.5 billion for European businesses and another \$500 million for U.S. and European service providers, according to a study by Ferris Research. Figuring it takes 4.4 seconds on average to deal with a message, the messages add up to \$4 billion in lost productivity for U.S. businesses each year. Another \$3.7 billion comes from companies having to buy more powerful servers and more bandwidth as well as divert staff time. The rest is attributable to companies providing help-desk support to annoyed users.

What to do

Spam has increasingly become a problem on the Internet. Unfortunately, most countries around the world currently have no adequate laws or regulations to control it. It is a very frustrating situation for users as well as for technical support personnel. It is a basic fact of Internet life that if you use the Internet, you will get unsolicited e-mail.

How to limit spam¹

Users of Outlook 2002: Click *File, New, Folder* to create a folder to store spam. Name it *Spam, Junk Mail* and click *OK*. Choose *Tools, Rules Wizard*, click the *New* button, and click *Next*. Uncheck *from people or distribution list*, check *where my name is not in the To box*, and click *Next*. Click the specified hyperlink in the 'rule description' field, browse to the folder you created, click *OK*, and then *Next*. Check *except where my name is in the Cc box* and, optionally, *except if from people or distribution list* and *except if sent to people or distribution list*.. Click *Next*, give the rule a name if you want to, and then click *Finish*.

Users of Outlook Express 6: Create a spam destination folder (*File, New, Folder*), name it *Spam* (for example), and click *OK*. Next, choose *Tools, Message Rules, Mail*, and click *New*. In the Conditions list box, scroll to and check *Where the To or CC line contains people* and, optionally, *Where the From line contains people*. Click the resulting *contains people* link in the Rule Description box, and fill in your e-mail addresses, mailing lists, newsletters. Then click the *Options* button, select *Message does not contain the people below*, and then click *OK* twice. Finally, check *Move it to the specified folder* in the Actions list box, click the *specified* link in the Rule Description box, and click *OK* twice to save the rule.

Users of Mozilla 1.x/Netscape 7.x: Create a spam folder, give the folder a name, and then choose *Tools, Message Filters*. Click *New*, and enter a name for the filter, then select *to or CC* in the first drop-down list of criteria, and choose *doesn't contain* in the second list. Type your e-mail address in the last field on the line. Click *More* to enter additional filter criteria. Choose *Move to folder*, select the spam folder that you just created in the last drop-down lists, and then click *OK* twice to save the filter.

Tips to reduce SPAM

- Avoid posting your e-mail address online.
- Don't list your e-mail address directly on a Web page
- Don't use e-mail addresses that are easy to guess
- Never respond to spam.
- Block unwanted e-mails from a specific spammer using filters inside your e-mail program.
- Pay attention when filling out online forms and disable the checkbox (usually enabled by default).
- Before you sign up at a web site, find out about that site's privacy policy.
- Use the Maps Real-Time Blacklist available [here](#).
- Sue the spammers: AOL has won almost \$7 Million in a Spam Case presented [here](#).
- Switch to an Internet provider offering spam filtering.

¹ Always remember to CONSULT with your system administrator before executing these changes.

How does RAV AntiVirus fight spam?

GeCAD Software is a company dedicated to its customers: your problems are our problems. And this is not just a way of speaking: we too receive spam! Therefore, we have looked for a solution to fight this flagellum. And we came up not with just one, but with several solutions.

RAV Engine, the main component included in all RAV AntiVirus programs, includes starting with its version 8.9 an **AntiSpam** module. This module has been included first in our **RAV AntiVirus for Mail Servers** products and we are currently working on including the module in all the **other** products of ours.

How does the Antispam work in RAV AntiVirus for Mail Servers?

When a mail message reaches a RAV-protected mail server, it is first confronted with the **White/Black List (WBL)**. This is a static configurable list that any system administrator can use for specifying the mail addresses from which he wants to automatically **accept** messages (**Static White List**) or the mail addresses from which he wants to automatically **reject** or **discard** messages (**Static Black List**).

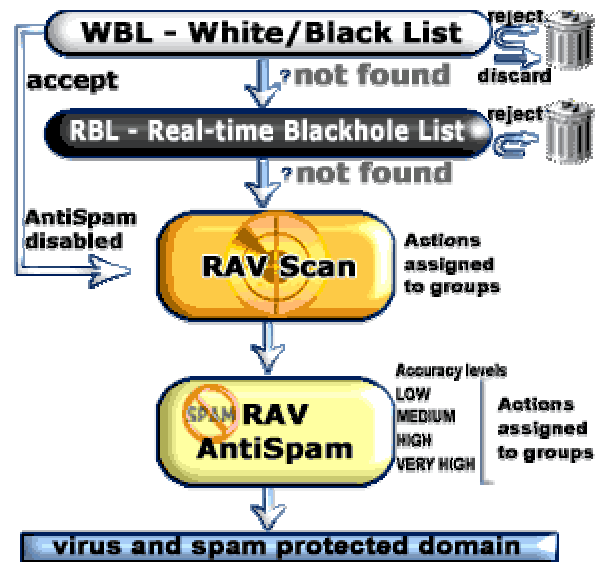
If the mail just received by the RAV-protected mail server comes from an address found in the **Static White List**, then the search in the **RBL** is not executed anymore and **ravmd** jumps directly to the scanning process for the respective mail. Also, the antispam module is not used for the mail coming from addresses found in the **Static White List**. If the mail just received by the RAV-protected mail server comes from an address in the **Static Black List**, the mail is automatically **rejected** or **discarded** (according to the specified settings).

If the address is not found in the **White/Black List (WBL)**, the mail is confronted against the **Real-time Blackhole List (RBL)**, a dynamic list with sites containing listings of known spammers. If any of the IP addresses from the mail's header is listed on one of the websites defined in this list, the mail is automatically rejected. Otherwise **ravmd** jumps to the scanning process for the respective mail. The system administrator can of course choose not to use these **WBL** and **RBL** features.

Assuming the mail is passing OK through the virus-scanning process (i.e. the message is clean or **ravmd** has cleaned it), the antispam search is executed. **ravmd** is looking for patterns known to be specific to spammers on the **Header** and **Body** levels of the mail message. Depending on its specifics, the mail message is classified in one of the following **accuracy levels**: **Low**, **Medium**, **High** and **Very High**.

For each of the four accuracy levels specified above you can configure different strings and separate actions to be used/taken by **ravmd**.

Don't be scared by all these parameters and actions: a default (operational) configuration is included in your setup program. Also, all the corresponding parameters are explained in details in the *User Guide* available [here](#).



Useful links

<http://spam.abuse.net/> - A group actively engaged in fighting spam for years. Available to the public since 1996.

<http://www.junkbusters.com/> - One of the best sites for information on spam and other privacy invasion issues.

<http://www.spamcon.org/> - Laws, anti-spam information, and links to other resources

<http://www.stop-spam.org/> - lots of technical information on how to fight spam.

<http://www.cauce.org/> - Coalition Against Unsolicited Commercial Email

<http://www.howtofightspam.com/> - If you're new to the fight against spam, this site is for you.

<http://www.spam-archive.org/> - A sophisticated, indexed, searchable database to Junk EMail collected from around the world.

<http://www.imc.org/imc-spam/> - Group dedicated to solving the unsolicited bulk email problem.