



Guide to Controlling Spam

COPYRIGHT NOTICE

This work is licensed under the Creative Commons Attribution License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Disclaimers

While the material in this report is intended to be as accurate and timely as possible, [Productivity Portfolio](#) makes no warranty or guarantee concerning the accuracy or reliability of the material at other sites to which this report links. The links are provided for convenience only.

Publisher's Note – 04/16/2005

The material you are viewing is a subset of a guide that was released in 2003. That guide was 120 pages and contained over 20 different product reviews. Since that time, many of those products have changed. Some companies have been acquired and countless new ones have appeared. As a result, we felt it was best to remove the product review section since we did not have the resources to test these products.

We took the remaining pages and broke them into separate sections that people could download. These include:

Section 1: **Introduction**

Section 2: **User Prevention** – this section provides actionable steps you can do now to limit additional spam.

Section 3: **Methodologies** - this section highlights the major methods used to detect spam.

Section 4: **Questions to Ask** – this section provides some questions that can assist you in making a product selection.

Section 5: **Features** – this section provides a summary of features we found in the products we reviewed.

Section 6: **Types of Solutions** – this section lists the types of solutions we tried and our comments on strengths and weaknesses.

Section 7: **Resources** – listing of other web sites that have spam and product information.

Section 8: **Glossary**

Types of Solutions

Below are descriptions of the various product types we reviewed. You'll notice that some products are listed several times as they have features that overlap. These products are marked with an asterisk (*) to indicate multiple listings.

Internet Service Provider Solutions

The first step you may want to take is to contact your ISP to see what features they offer. Many ISP have services ranging from additional mailboxes to filtered email. Unfortunately, we found ISPs do not always inform customers or prospects of these services.

If you're shopping for an ISP, you can get a sense of how concerned an ISP is about spam by viewing their end user license agreement (EULA) and Privacy policy. Some ISPs make casual references to spam whereas others put the user on notice that spam will not be tolerated.

Additional Mailboxes

One simple solution is to ask your ISP for an additional email address as many plans allow for multiple mailboxes without extra fees. This solution is good for segregating email. One account can be used for primary contacts such as friends, family and business colleagues. The second account can be used for newsgroups, product registrations, etc.

ISP Spam Filters

As mentioned earlier, some Internet Service Providers offer spam filtering. Sometimes this feature is part of a bundled service that includes virus detection. In many cases, the feature is part of the monthly service fee although some ISPs charge for these services.

Although each ISP solution we reviewed filtered spam, their effectiveness varied considerably, mostly by design. As with blacklists, the way an ISP implements the solution can influence your decision. For example, Brightmail excels at ensuring flagged email is truly spam. However, this approach allowed more spam into your Inbox. Postini approached the situation from another perspective and concentrated on preventing questionable mail from reaching your Inbox. This approach quarantined more email that is legitimate. Both approaches are effective, but require the user interact differently to make them effective for their needs.

One difference with an ISP solution is support. In theory, the customer should benefit from “one stop” support. However, we found the support people with national ISPs were not as versed on their spam filtering products. In contrast, support personnel for smaller ISPs were very effective in resolving our questions and problems.

Each of the ISP solutions separated spam into a folder that is accessible from the web. Some people prefer this approach as it saves time when downloading email. Others dislike the feature, as they have to log into a separate area with their browser. These people were also more apt to forget to check the spam folder.

We reviewed three ISP spam filters and believe them all to be worthwhile tools for any subscriber. Although these services are not as robust as stand-alone programs, they provide reasonable spam protection with minimal user effort. These products may also appeal to users who prefer web based email or users who access their email from multiple locations and devices.

Reviewed Products:

- [Brightmail](#)
- [Postini](#)
- [SpamAssassin](#)

Filtered Email Accounts

Most of these products are web-based and allow for larger email storage. These services provide users with a separate email account, but they don't provide access numbers to the Internet. Since they are email providers, they tend to have strong email features in addition to spam filtering.

These accounts work well for people who access the Internet from work, but prefer having their personal email on another system. These systems also work for people who prefer having email kept on a server instead of their local machine.

As with ISP solutions, the spam filtering is automatic and requires little user setup. The service provider takes care of all the maintenance aspects and automatically updates the spam rules or engine as needed. These services tend to do a better job of integration with the quarantine area.

Another benefit is each of these services allowed the user POP access. This means you could also use your email application such as Outlook etc to access the email.

Reviewed Products:

- [SpamCop](#)
- [Mailshell*](#)

Email Forwarders

A less publicized option in controlling spam is to use an email forwarder that filters email as part of their service package. If you're not familiar with mail forwarders, they take your email and then forward it to one or more email addresses. For example in our testing, we used our primary email address from POBOX and forwarded our email to five different email accounts.

While this report doesn't review email forwarders, you can find a listing of services in the Resources section of this guide.

Disposable Email Addresses (DEA)

One of the more interesting solutions we reviewed was disposable email addresses. These are email addresses used for temporary purposes and then discarded. At first, we dismissed the idea since we already had spam-filtering programs. And technically speaking, these services don't filter spam. However, we failed to realize that the major benefit of these addresses is they protect your main email address. This benefit became apparent to us after we signed up for a trade show using our primary email address. Shortly after registering for the trade show, the promoter sent our email address to over 100 exhibitors. Unfortunately, we have no idea what these vendors will do with our registration information, but we can expect to get product announcements and special offers from them and their marketing partners. In hindsight, we should've used a DEA to protect our main email address.

One of the other benefits of DEA providers is they allow you to track the use of your disposable email address. For example, had we used a DEA for our trade show registration, we could've added a code indicating "XYZ Trade Show". We would then know that all email to that address was a result of the show registration. If we received email to that address from someone other than an exhibitor, we can assume our email address was sold or exchanged. This can be a fascinating process to see how your email address gets out into the wild. Just

for fun, you might look at [Spamdemic Map](#) to see the relationships between various companies and advertisers.

The downside to using DEAs is minimal. The first issue is you need to be careful when replying to email. If you don't follow the vendor's suggestions, you could mistakenly expose your real email address. For example when using a DEA, you should change your email signatures to include your disposable email address. The same caution applies to reporting spam with these addresses. If you're not careful, you may accidentally report the wrong party.

Reviewed products:

- [Mailshell*](#)
- [Spam Motel](#)
- [Spamex](#)

Email Filters

We appreciate email rules as they allow you to define what to do with emails matching defined criteria. If you don't get a lot of spam, you may find it easier to define email rules within your email program and move suspected spam away from your Inbox. Before our spam problem became unmanageable, we simply used an email rule that moved any email that didn't include our email address in the To: or CC: line to a separate folder.

Although time did not permit us to test this category, there are numerous programs available from popular download sites such as [Snap Files](#), [c/net](#) or [TUCOWS](#). One of the popular programs is [MailTalkX](#) by SoftByte Labs.

Below are some links from Microsoft and the Help Desk at George Washington University that can assist you in creating email rules.

Outlook

[How to filter junk and adult content e-mail messages in Outlook 2002](#)
[How to Filter Junk Email and Adult Content for Outlook 2000](#)
[How to Filter Junk Email and Adult Content for Outlook 98](#)
[Junk Email Filters for Outlook](#)

Outlook Express

[Creating Email Rules in Outlook Express](#)

Netscape

[Mail Filtering for Netscape Messenger](#)

Stand Alone Programs

These programs work outside of your email program and interact with your mail server. In other words, they don't pull down the entire email from the server to your computer. This approach is beneficial for several reasons. First, you save time and space since you don't have to download all your email. You can generally delete spam messages directly from these programs. Secondly, by not downloading the email, you limit your exposure to any viruses associated with these emails. Lastly, these programs can operate in the background and alert you to any new email without keeping your email program open.

One disadvantage to these programs is the integration with your email application. Although these programs may launch your email application, they generally don't have the ability to view the entire message or allow you to respond directly to an email.

Another disadvantage is some of these programs can compete for email with your regular email application. This problem is called "race condition" and can occur if both programs are open and set to retrieve emails on an interval basis.

Reviewed products:

- [Choice Mail*](#)
- [Mail Washer*](#)
- [Norton Internet Security](#)
- [SpamKiller*](#)

Application Add-in Programs

These programs are designed to work with your email programs such as Outlook, Outlook Express or AOL. The programs are tightly integrated with the email readers and often add a toolbar or menu to the email application.

As a result of this integration, these programs are sometimes limited by the underlying application. For example, Outlook Express doesn't have the same structure as Outlook and is much harder to integrate email rules. In addition, these spam filtering programs are usually locked into the existing data structure and don't provide additional information such as why the email was flagged. However, they all do an excellent job of creating a whitelist since they leverage the email application's address book.

Another issue with Add-in programs is they may interfere with the underlying program, your personal rules, or some other Add-in application. An example of this type of conflict occurs with Outlook and ActiveSync. ActiveSync is a required component for the Pocket PC. However, certain Outlook Add-in programs will not load because of this relationship. Microsoft has acknowledged this issue in their [knowledgebase](#).

Most Outlook Add-in vendors prefer you only install one Add-in since problems may arise when multiple modules are installed. Sometimes these issues can be resolved by changing the load order. In our testing, we found some Outlook Add-in programs worked fine with other modules and some displayed erratic behavior. Similar problems can also occur if you use Microsoft Word as the email editor for Outlook.

Another issue with Outlook concerns Outlook rules that may affect your results. Some add-in programs take precedence over your own Outlook rules. For example, you might have an Outlook rule that states any email from flyingmonkey@blueappleseed.net should go to your Humor folder. If your spam filter classifies the email as spam, the email will go to the designated junk mail folder. However, other programs will not even look at this email since it's not going to the Inbox.

It's also important to note that even though these products leverage the email program's address book; your whitelist can still get out of sync. Most of these programs build your whitelist using the existing address book, but any changes may have to be manually added to your whitelist.

Reviewed products:

Outlook

- [iHateSpam for Outlook](#)
- [MailFrontier](#)
- [SpamCatcher](#)
- [Cloudmark for Outlook](#)

Outlook Express

- [iHateSpam for Outlook Express](#)
- *Note: On 2/5/03, [MailFrontier](#), the producers of Matador, announced a product for Outlook Express. The product is still in beta.*

America Online

- Spam Inspector for AOL (Discontinued)

Permission and Email Challenges

Permission and Challenge email systems are a new and interesting approach to fighting spam although they can be rather exclusionary. As with many spam solutions, you define whom you want to receive email from. Anyone not defined on your acceptable list either is turned away, or receives a message with instructions on how to contact you. This method works in part because spammers don't take the time to fill out the required information.

While we believe these systems can be very effective, we think they'll be controversial. The success of these programs is dependent on several factors.

1. The set up process needs to prompt the user for as many whitelist entries as possible.
2. The challenge messages have to be viewable by all email readers. There has to be a text alternative.
3. You can expect that some people will not respond to these requests because of time, resources, or distaste for such systems.

Reviewed products:

- [Choice Mail*](#)
- [MailFrontier*](#)

Web Based Email

We also quickly reviewed the built-in features and controls of the large web-based email providers. Our initial intent was to provide full product reviews. However, we decided against this as we found the feature sets to be inadequate. Instead, we would encourage people to supplement their service with spam filtering programs that work with these providers. Lastly, we would remind people that most of these services have marketing preferences that could increase the number of unwanted emails.

There's no question that these large services attract spammers with all sorts of dictionary and algorithm tools. We were amazed at how many spam emails we received on these accounts in such a short time span. The majority of these spams were easy to spot as they included our account name in the Subject: line. With the exception of AOL, we were at least able to create a custom rule to move any email containing our account name into a folder other than our Inbox.

AOL

About the nicest thing we can say about the enhanced email features of AOL 8.0 is they've added a "Report Spam" button and several sort groups. Supposedly, the service has improved junk filters, but we didn't see any evidence of this. Moreover, the service still does not allow members the ability to create email rules. Instead, the user must use various "Mail Control" features to limit access to their email account. For people that have to use AOL, we would encourage you to use a separate screen name for chat and instant messaging.

Supplemental Products:

- [Mailshell*](#)
- Spam Inspector for AOL (discontinued)

In addition, you might want to investigate [AOL2POP](#). This new utility converts your AOL email to a POP3 format so you could use other email applications such as Outlook, Outlook Express, Eudora, etc.

Hotmail

You can reasonably figure that a service that receives over a billion emails a day will have spam. The situation should improve shortly as Microsoft recently announced an agreement with Brightmail. In the interim, users can use Hotmail's custom filters.

Aside from spam, Hotmail also provides opportunities for fraud. We should caution users that we saw one instance of a web-based service claiming to clean your Hotmail Inbox of spam. Apart from the free trial, we saw little contact information about the company. Although there is nothing of value in our Hotmail account, someone could make use of our password and account name to generate email on our behalf. We would strongly encourage users to check the validity of such companies before revealing your email account name and password.

Supplemental Products

- [Mailshell*](#)

- [SpamKiller*](#)

MSN

Microsoft recently released version 8.0 of MSN with the usual flare we've come to expect. We were hopeful that MSN Junk Protection would provide relief from spam. Unfortunately, we found their neural network missed the mark and didn't catch much spam. According the MSN help file, the system requires 200 unique messages identified as "Junk" and 200 unique messages identified as "non junk". We definitely exceeded these counts on the same test machine and yet we saw minimal improvement in their system. However, we have seen reports on the web where some users indicate their spam problem has been reduced with the new software. In addition, we spoke to some experts who indicated it realistically takes several thousand emails for these neural network or Bayesian systems to be truly effective.

MSN 8.0 has also muddied the water somewhat for existing customers. Users who previously had POP3 access are automatically switched to HTTP email during the MSN 8.0 installation process. As a result, you'll see some products indicate they work with MSN, but this may not include MSN 8.0

Supplemental Products

- [MailWasher*](#)
- [SpamKiller*](#)

Yahoo!

The last service we looked at was Yahoo! Some of us have had the free Yahoo! account for years and have been amazed at how little spam we receive. Still others complained loudly that their Yahoo! address attracts too much spam.

While Yahoo! does have a framework for building rules and lists, these features are limited in number unless you upgrade to their paid account. For a free email account, they provide a nice array of features, but excel at none. While we wouldn't rely on using any free email service as a primary email account, they can be used effectively for newsgroups.

Supplemental Products

- [Mailshell*](#)

On the Horizon

As with any writing project, things change as you're well into the writing. We encountered numerous product versions and pricing changes. One interesting development was a methodology called Bayesian Filtering that is receiving a fair amount of press. As the other products mentioned, these solutions won't stop spam unless they dramatically alter the economics. However, these new products will assist in identifying spam.

Bayesian filtering is a statistical approach to solving the spam problem. Most of the research has been conducted by [Paul Graham](#). The process starts by analyzing the words and tokens within a user's email (spam and non-spam) including headers. From this email sample, a probability algorithm determines how likely these items are contained in real email versus spam. Over time, these systems become very accurate at predicting whether your email message is spam. The advantage is that the analysis is done on your email. The downside is that the system requires some work on the user's part to identify which emails are good and which are bad until the system can accurately predict. This learning process is gradual and dependent on how much email you receive.

During the course of writing this report, we've noticed a large number of new products using this method. Many of these products are in the early developmental stages and some are for administrators. If you're interested in this method, we'd suggest the following links:

A Plan for Spam – article written by Paul Graham
www.paulgraham.com/spam.html