



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**

User Prevention

Even if you use one of the solutions mentioned in this report, it won't completely fix your spam problem. These solutions are primarily designed to pre-process your email and move spam away from your Inbox. Although getting a new email address can limit spam for the short-term, spammers will eventually find the new mailbox. However, there are steps you can take now to prevent new instances of spam.

Some of the spam you receive *may* be a result of your actions such as:

- posting to newsgroups with your real email address
- entering sweepstakes or contests
- registering products
- replying to "unsubscribe" instructions
- posting your email address on your web page

1. Use an alternate email address for newsgroups, contests and web registrations

Many websites require you to submit an email address to receive services or additional information. If you don't plan to correspond with these people on a regular basis, provide an alternate email address. This way if your email address is harvested or compromised, it's not your primary address. You need to ask yourself why someone needs your email address and what he or she plans to do with it.

You can get free email accounts from [Yahoo](#) or [Hotmail](#). You can also check with your current ISP to see if they provide additional email addresses.

Another option is to use disposable email addresses (DEA). As the name suggests, these are email addresses you can turn off or delete if spam appears. Most DEA providers also forward your DEA email to your primary email address. A listing of providers can be found in the DEA section of this report.

2. Thoroughly read a company's privacy policy and end user license agreement (EULA)

Most websites state their policies for sharing data. Although these pages contain complex language, you should review this information to see how your data is handled. This is particularly true for free services. Many of these businesses share or sell your data with third parties as part of their business model. These policies also assume consumers want emails and require them to "opt-out" from receiving email.

Since policy pages are often long and display in a separate window. We often copy and paste the text into Microsoft Word. This allows us to print and read the policies before we accept the terms. We also save the document so we have a copy of the policies at the time we subscribed to the service.

Here are two examples we copied from a popular lotto site and a free email forwarder. (We removed the original company names and substituted AcmeOnlineWidgets.)

(Example 1)

Limits of Confidentiality

As part of its day-to-day business activities, AcmeOnlineWidgets.com may disclose certain information about AcmeOnlineWidgets.com Players to certain third parties, principally:

- (1) AcmeOnlineWidgets.com's Partners;
- (2) Marketers who use AcmeOnlineWidgets.com's network of Players; and
- (3) third parties who provide services to AcmeOnlineWidgets.com;
- (4) AcmeOnlineWidgets.com's advertisers.

(Example 2)

AcmeOnlineWidgets.com Privacy Notice and Choices:

The policy of AcmeOnlineWidgets.com is to protect the privacy of AcmeOnlineWidgets.com Members who are using any of the AcmeOnlineWidgets.com Services. Please be aware, however, that as a condition of membership and use of the AcmeOnlineWidgets.com Services, AcmeOnlineWidgets.com requires Members to select areas of interest and thereby agree to receive marketing materials from AcmeOnlineWidgets.com or third parties related to those interests. Members may choose at any time to opt-out of mailings on their profile, including during registration and when they receive any third-party mailings from AcmeOnlineWidgets.com; however, AcmeOnlineWidgets.com reserves the right to cancel the membership of Non-Premium Users in the event such a Member chooses to completely opt-out of all mailings.

Both examples indicate what you can expect by subscribing to the services. If you've accepted these terms, you've also opened the door to additional email. Furthermore, since you accepted their policies, these organizations don't consider the email they or their partners send as spam.

3. Know how to respond to spam.

Frequently spammers use tools that assemble large lists of email recipients based on dictionaries and ISP domains. This is why you sometimes see emails with numerous addresses in the TO: fields that differ slightly.

Although the spammer's primary goal is to sell goods, a second goal may be to harvest a list of valid email addresses. These lists can be exchanged or sold to other spammers. One way spammers verify an email address is by adding "Unsubscribe" instructions to their emails.

We are strongly against sending unsolicited emails to those who do not wish to receive our special mailings. You have opted in to one or more of our affiliate sites requesting to be notified of any special offers we may run from time to time. We also have attained the services of an independent 3rd party to overlook list management and removal services. This is NOT unsolicited email. **If you do not wish to receive further mailings, please click this link.** Please accept our apologies if you have been sent this email in error. We honor all removal requests

Unfortunately, clicking an Unsubscribe link also informs the spammer of a valid email address that is in use. Do not assume that because you received the email, the spammer knows your email address is valid.

While we believe you should unsubscribe to a newsletter or organizations you recognize, we suggest you ignore items such as the example below. If the sender were serious about complying with Federal requirements, they should know there is no such [bill](#). We also wouldn't put too much faith in them reporting you as a spammer.

This message is in full compliance with U.S. Federal requirements for commercial email under **bill S.1618 Title 111, Section 301**, Paragraph (a) (2) (C) passed by the 105th U.S. Congress and cannot be considered SPAM since it includes a remove mechanism. Further transmissions by the sender may be stopped at no cost to you by clicking on [here](#) .

We practice responsible mailing by honoring all remove requests, following all U.S. laws, and oppose spamming. If you complain and have the remove address closed you are doing a disservice to other receivers of this message since they will have no mechanism to be removed from future mailings. **In addition, this message is in strict compliance with U.S. law so if you flame the 'chyna@hop.to' we will report you to your ISP as a SPAMMER, which will result in your account being closed.**

We've also heard reports that some spammers are using a reverse strategy where the provided link isn't for unsubscribing, but for opting-in. These spammers are hoping that you won't notice the wording difference.

If you don't know the organization sending the email and a product or service is represented, we suggest sending the full email item, including header information, to the [Federal Trade Commission](#) at spam@uce.gov. Although many spam reporting organizations exist, the FTC reviews these emails for fraud.

Recent reports also suggest spammers are sending emails for the purposes of credit card and identity theft. This is particularly true of emails announcing low mortgage or interest rates. A naive consumer will contact the firm and answer a few simple questions by phone or web form. The spammer now has additional data such as full name, address, phone, social security number etc. These phone reps excel at "social engineering" which is the art of getting people to give up information.

4. Contact the Direct Marketing Association (DMA)

The DMA, a trade association representing marketers, offers some free services to consumers regarding print and email lists. To find out more about their services, including list removals, check the link below.

<http://www.dmaconsumers.org/consumerassistance.html#mail>

5. Scramble your Email address on your Web page

One of the items offered by many ISPs is your own web page. It's an opportunity to share with the world information about our friends, family, hobbies, etc. It also provides an opportunity for automated agents or "bots" to harvest your email address from the HTML page and add it to a list.

One safeguard is to use one of the utilities that scrambles or obfuscates your email address. These utilities take a typical MAILTO: reference such as

`Email`

and changes it to

`Email`

The new link still works, but many of the tools spammers use will have problems with this scrambled reference. Keep in mind, this solution is temporary, as some tools can decode these references. Another option is to use CGI scripts or web forms. A listing of utilities can be found in the Email Obfuscators part of the Resources section.

6. Check Your Web Browser

In rare cases, your web browser may pass along your email address. This was more of an issue in the early days of the web. All the same, you may want to verify your privacy by using the following web resources.

[Junk Busters Privacy Test](#)
[PC Flank Browser Test](#)