

# ANTI-SPAM TIPS

20081023dg

## Tips on How to Reduce or Eliminate SPAM

Spam, spam and spam. How to avoid spam, how to filter spam, and how to complain about spam are the items on this menu of junk mail fighting tips.

Heading (hyperlink) Short Description	Pop-Up long description
<p><b>Don't Use Your Primary Email Address to Sign Up for Anything</b></p> <p>You never know what might happen to an email address you use to sign up for Web sites or newsletters. It might be passed on to spammers.</p>	<p>Many web sites require you to sign up to access their services. Often, you need to provide a valid email address (to which your password will be sent, for example) during the sign-up process.</p> <p>There's nothing wrong with that. But you never know what will happen to the email address you give to the site.</p> <ul style="list-style-type: none"><li>• Hackers may break into the network and steal the email address,</li><li>• it may leak to the web due to some mishap, or</li><li>• it might even get sold to spammers.</li></ul> <p><b>Don't Use Your Primary Email Address to Sign Up for Anything</b></p> <ul style="list-style-type: none"><li>• This is why it's a good idea not to use your primary email address when you sign up at a web site.</li><li>• Use a disposable email address instead, an account at one of the <a href="#">free web-based email services</a>, or another secondary email address that is not critical.</li></ul>
<p><b>Assume Mail from Unknown Senders is Spam</b></p> <p>I don't know you... you must be a spammer! Here's how to use your email address book to identify and filter spam.</p>	<p>People who know you do not spam you. They may terrorize you, but they never spam you. Usually, these people are in your email client's address book. If they are not there yet, you should probably add them, because such an address book of everyone you know can be a helpful tool to identify spam. If you do not usually receive mail from strangers, you can assume that</p> <ul style="list-style-type: none"><li>• every message not from somebody in your address book is spam and</li><li>• filter such messages to the <i>Junk Mail</i> folder.</li></ul> <p>Now and then, you should check this folder for important messages you may have missed, maybe because somebody's email address has changed.</p> <p>Building on this idea of only allowing known senders, challenge/response spam filters render your email virtually spam free with very little to no maintenance.</p>
<p><b>Don't Believe Spammers When They Say "You Requested"</b></p> <p>You requested this tip, believe me. Spammers try to convince you that you requested their stuff, too.</p>	<p>There are two words that you will find in almost any unsolicited bulk email: "<b>you requested</b>".</p> <p>Don't believe it.</p> <p>Spammers count on your uncertainty, and that in doubt you will rather not take any action and complain about the spam.</p> <p>Chances are, however, that</p> <ul style="list-style-type: none"><li>• you did not request anything,</li><li>• especially if</li><li>• there is nothing about the company or person sending you bulk email you recognize, or if the service offered does not sound like something you would ever be interested in or request.</li></ul>

## **How Spammers Get Your Email Address**

Why spam finds you everywhere. The techniques employed by spammers.

Spam is amazing. In an unprecedented and astonishing effort, junk email reaches almost everybody online. All it takes to get on the mailing lists used by spammers is an email address. There is no need to sign up for anything or ask for emails. The spam just starts coming, out of nowhere, apparently without any plan, and without a reason. It invades email addresses that are never used.

But how do spammers discover email addresses? How do they find your mailbox when your best friend does not?

### **Dictionary Attack**

Big free email providers like Hotmail or Yahoo! Mail are a spammer's paradise, at least when it comes to finding spammable addresses.

Millions of users share one common domain name, so you already know that ("hotmail.com" in the case of Hotmail). Try to sign up for a new account and you will discover that guessing an existing user name is not difficult either. Most short and good names are taken.

So, to find email addresses at a large ISP, it's enough to combine the domain name with a random user name. Chances are both "asdf1@hotmail.com" and "asdf2@hotmail.com" exist.

To beat this kind of spammer attack,

- use long and difficult addresses.

### **Brute Searching Force**

Another tactic employed by spammers to discover email addresses is to search common sources for email addresses. They have robots scanning web pages and following links. These address harvesting bots work a lot like the search engines' robots, only they're not after the page content at all. Strings with '@' somewhere in the middle and a top-level domain at the end are all the spammers are interested in.

While not picky, the pages the spammers are particularly keen to visit are web forums, chat rooms and web-based interfaces to usenet because lots of email addresses are likely to be found there.

This is why you should

- disguise your email address when you use it on the net or, better yet,
- use disposable email addresses.

If you post your address on your own web page or blog, you can

- encode it

so visitors who want to send you an email can see and use it, but spambots cannot. Again,

- using a disposable address

provides a very effective and at the same time convenient alternative.

### **Worms Turning Infested PCs Into Spam Zombies**

To avoid being detected and filtered, spammers seek to send their emails from a distributed network of computers. Ideally, these computers are not even their own but those of unsuspecting users.

To build such a distributed network of spam zombies, spammers cooperate with virus authors who equip their worms with small programs that can send bulk emails.

Additionally, these spam sending engines will often scan the user's address book, web cache and files for email addresses. That's another chance for spammers to catch your address, and this one is particularly difficult to avoid.

The best anybody can do is

- keeping their email program updated and patched,
- being vary of any attachments they did not request and
- doing virus scans with a free, up to date scanner regularly.

<p><b>Ignore Delivery Failures of Messages You Did Not Send</b></p> <p>If you wonder why you are getting delivery failures for messages you know you did not send, the cause may be a worm or a spammer, and it's probably not on your computer.</p>	<p><b>Why Spammers and Virus-Generated Mail Use Fake From: Addresses</b></p> <p>For totally understandable (and entirely unacceptable) reasons, spammers rarely send their unsolicited messages using their own email address in the <i>From:</i> field. Not only would this reveal their identity, it would also allow you and the millions of other recipients to write angry replies. (You can still find out where the email originated, though, and complain to the spammer's Internet Service Provider.)</p> <p>Authors of worms and viruses desire the opposite to what spammers want, but the result is similar. For worms to spread, social engineering is important, and a crucial point is that the malicious code appears to come from a friendly or even trusted source.</p> <p>At the same time, the <i>From:</i> line should not contain the email address of the infected computer's owner. The reply from a virus filter notifying them that their computer was infested could alert them. That's why worms put real, but random addresses in the <i>From:</i> line. They usually pick them up from the email clients' address books.</p> <p>For both spam and worms don't care who the recipients of their — hopefully millions — of replicas are, the messages often go to email addresses that are inactive, full or have never existed.</p> <p><b>When, How and Why Delivery Failure Reports are Generated</b></p> <p>Since email delivery usually works (or at least did before overzealous spam filters started blocking legitimate mail), success is not normally reported but failures are. If you have ever mistyped an email address I'm sure you know the often detailed, not always easy to parse but usually alarming "delivery failure" messages.</p> <p><b>Ignore Delivery Failures of Messages You Did Not Send</b></p> <p>Now, what happens if a spammer or a virus decides to put your email address in the <i>From:</i> line can be annoying, disturbing or disastrous. If the messages claiming delivery failures of messages you did not author (sometimes, these bounces of messages you did not send are called "backscatter") don't come in the thousands,</p> <ul style="list-style-type: none"> <li>• it is usually best to ignore them.</li> </ul> <p>There is little you can do. (If one of the return messages includes the complete headers of the bouncing mail, you can parse them using a spam analysis tool like SpamCop to find where it originates and then inform the ISP that one of their users has a virus. I don't recommend that, though. It will be of little use and consumes additional time and resources. In the case of returned spam, it can be useful to alert the ISP where it originates, though.)</p> <p><b>Scan Your Computer for Viruses and Worms Nevertheless</b></p> <p>If you do not have a virus scanner installed and can't rule out that your computer is infected by a worm or has been turned into a spam zombie,</p> <ul style="list-style-type: none"> <li>• check your system for viruses (for free)</li> </ul> <p>before ignoring the delivery reports.</p> <p>If your get a few hundred of the delivery failure messages per minute, you should inform your ISP so they can filter them out to avoid having your mailbox clogged.</p>
<p><b>Mail not Addressed to You is Likely Spam</b></p> <p>They didn't want to reach you, anyway. Mail where you don't know the sender that which is not addressed to you is likely spam.</p>	<p>There is hardly an unsolicited mass email message that has your email address in the <i>To:</i> or the <i>Cc:</i> field.</p> <p>This is why you can set up a filter that</p> <ul style="list-style-type: none"> <li>• moves all incoming messages that do not carry any of your email addresses in either the <i>To:</i> or <i>Cc:</i> field to the "Probably Spam" folder.</li> </ul> <p>Of course, you should have filters that catch all mail from mailing lists before the not-addressed-to-me filter triggers.</p>

<p><b>Don't Buy from Spammers</b></p> <p>Spammers are in it for the money. Here's what you can do (and should not do) to help make spam go away while letting email flow freely.</p>	<p>Spam works and exists because it is so cheap to send an email. Since the cost of sending bulk emails to hundreds of thousands of people is so low, it pays off if only a fraction of the recipients respond.</p> <p>Rising the cost of email is hardly an option. So it is important to never buy from spammers.</p> <p>Don't even visit their web sites or do anything else they want you to do. If there is no profit in spamming, all spammers that are in it for the money (and I bet all of them are) have an incentive to stop.</p> <p>Since spam is to some degree in the eye of the beholder, chances are nobody ever buys something responding to spam anyway, though. For those who buy, the message was targeted.</p> <p>The problem is actually not with those who reply to spam. The problem is that this targeting was achieved by simply mailing everybody.</p> <p>This is why we should probably reformulate this to read:</p> <ul style="list-style-type: none"> <li>• Don't buy from somebody you don't know (unless it is clear and you can be sure that they did not spam),</li> <li>• and from those you did not opt in for only if you can opt out easily.</li> </ul> <p>This is not to mean that Coca-Cola can spam everybody, and it is also not to mean that every unsolicited email is spam. It is my currently best shot at making sure spam doesn't work while email does freely.</p>
<p><b>Mail with "ADV" in the Subject is Spam</b></p> <p>Messages that have "ADV" in the Subject are likely spam (or would you use it in any message?).</p>	<p>Based on some legislative attempts to control spam, spammers sometimes include "ADV:" at the begging of the subject line to make their unsolicited message appear legitimate.</p> <p>You can safely assume that</p> <ul style="list-style-type: none"> <li>• any message that carries "ADV" in it subject is spam</li> </ul> <p>and set up a filter that either deletes it or puts it in your "Possible Spam" folder.</p>
<p><b>Messages Containing "One-Time Mailing" Are Spam</b></p> <p>One-time mailings get a one-way ticket to the trash.</p>	<p>Spammers usually want to tell you that their message is not spam.</p> <p>But even if they admit that a message is sent without solicitation, they try to tell you that there's no point in doing something against them. That's why they then say: "<b>This is a one-time mailing.</b>"</p> <p>Usually, it of course is not. But since <b>this phrase is used almost exclusively by spammers</b> it makes for a nice filter.</p> <p>Your anti-spam filters could look for "one-time mailing", "one-time-mailing", "onetime mailing" and other variations in the body of incoming messages and place matching messages in the "Possible Spam" folder.</p>
<p><b>Don't Delete Spam Automatically</b></p> <p>Make sure you get to see all the mail you want. Spam filters are not perfect, so they may produce false positives and delete legitimate mail.</p>	<p>Filtering spam is a tricky matter. While many clever strategies exist that can significantly cut down on the amount of unsolicited mail in your Inbox, no filter can be 100% accurate.</p> <p>There will be spam that slips through the filter or — worse — legitimate mail that's caught by the anti-spam filter.</p> <p>That's why it's a good idea to build a safety net into your filters.</p> <p>Do not delete mail immediately with an anti-spam filter, do not even put it in the trash.</p> <p>It's usually better to have a special "Possibly Spam" folder where filters put the suspected spam. Every few days you can have a look at the contents of this folder and, if it does not contain any legit email, empty it.</p>

<p><b>Don't Use "This is Spam" to Unsubscribe</b></p> <p>The "This is Spam" button is an easy and effective way to get rid of spam, but you should make sure you use it only for spam. Otherwise, bad karma may not be the only unpleasant consequence.</p>	<p>Many email services like AOL, Gmail, MSN Hotmail or Yahoo! Mail let you report spam using an easy to use <i>This is Spam</i> button. The <i>This is Spam</i> button is not only easy to use, it is also quite effective. The emails you report are used to tweak the spam filters so that they catch the type of email you reported in the future.</p> <p><b>Don't Use <i>This is Spam</i> to Unsubscribe</b></p> <p>This efficiency is the reason why you should make sure you</p> <ul style="list-style-type: none"> <li>• use the <i>This is Spam</i> button only for spam.</li> <li>• In particular, reporting newsletters you have once signed up for but don't want to receive any more can have negative consequences:</li> <li>• Others who have signed up for the same newsletter (and still want it) may not receive it any more because it's filtered away since you reported it as spam.</li> <li>• The opposite is also true: others may report your favorite newsletter using the <i>This is Spam</i> button and you may suddenly stop receiving it.</li> <li>• If the <i>This is Spam</i> button is used for lots of legitimate emails, the email service providers may get more hesitant about implementing any changes based on user submissions.</li> </ul>
<p><b>Watch Out for Those Checkboxes</b></p> <p>Make sure you don't opt in for emails you don't want, and watch out for checkboxes when you submit any form on a Web site.</p>	<p>When you sign up for something on the Web, there is often some innocent-looking text at the end of the form saying something like: "YES, I want to be contacted by select third parties concerning products I might be interested in." Quite often, the checkbox next to that text is already checked and your email address will be given to you don't know who.</p> <p><b>Watch Out for Those Checkboxes</b></p> <p>To avoid that,</p> <ul style="list-style-type: none"> <li>• look closely at every form you fill on the Web and</li> <li>• make sure all relevant checkboxes are not ticked.</li> </ul> <p>Sometimes, the text will read: "NO, don't give away my email address," and the checkbox will consequently be unchecked by default. Check it.</p>
<p><b>Spammers Track Usage, Too</b></p> <p>Here's another reason not to open spam: using embedded images, the spammer may watch you do it, and that may go down on your permanent please-spam-me-some-more record.</p>	<p>Most of the HTML newsletters you receive will include images, which are downloaded from a remote server when you open the email to track whether you actually do open (and possibly even read) the message.</p> <p>Spammers, never shy to exploit all possibilities, are using tracking images, too. Some do indeed seem to be interested whether an email address works, and by downloading the tracking image you confirm that (maybe resulting in even more spam).</p> <p>So how can you avoid being tracked?</p> <ul style="list-style-type: none"> <li>• If you can tell something is spam by the subject, the sender or the recipient, don't open it at all.</li> <li>• Additionally, you can configure your email client to avoid this kind of privacy infringement.</li> </ul>
<p><b>More Email Addresses Mean More Spam</b></p> <p>Spam behaves a lot like cars. Wherever you build a road for it will travel, and it will always fill up all the available space (and more).</p>	<p>No matter what you do, chances are spammers will find out about all your email addresses. And they'll not spam every address equally, but they'll spam them all a lot.</p> <p>That's why it's probably a good idea</p> <ul style="list-style-type: none"> <li>• not to use more email addresses than you need.</li> </ul> <p>The situation is somewhat analogous to roads and traffic: more email addresses will generate more spam like more roads will generate more traffic.</p>

<p><b>Stop Spam with Disposable Email Addresses</b></p> <p>Once your email address gets in the hands of spammers, you will get spam. Lots of it. Find out how to use disposable email addresses to dispose of spam (and spammers) effectively.</p>	<p>You've read it and you know it well: using your real, primary email address anywhere on the web puts it at risk of being picked up by spammers. And once an email address is in the hands of one spammer, your Inbox is sure to be filled with lots of not-so-delicious spam every day.</p> <p><b>Stop Spam with Disposable Email Addresses</b></p> <p>But what should you use instead of a real email address?</p> <ul style="list-style-type: none"><li>• Use disposable email addresses!<ul style="list-style-type: none"><li>○ Never insert your real email address in a form on the Web. They might spam you or, worse, give your address to spammers. Use a disposable address instead, and choose from a number of services that offer them.</li></ul></li></ul> <p>A disposable email address will forward all mail to your real address. So where exactly is the benefit? Won't it forward all the spam, too? Not if you dispose of it.</p> <p><b>What To Do When You Get Spam</b></p> <p>As soon as you get spam through a disposable address, you disable it, and all messages (and all spam) sent to the disposable address bounce back to the sender instead of your Inbox.</p> <p>Since (and this is a crucial point) you give every disposable email address to precisely one web site or contact, you know exactly who spammed you or leaked the address to spammers.</p> <p>For the same reason turning off a disposable address has no impact on all the other mail you receive through your real address and (preferably) other disposable email addresses. You merely stop the spam.</p> <p>You can even use disposable email address to stop spam you get from posting your email address on your home page or blog in a mailto link.</p>
<p><b>Submit Spam to SpamCop via Email</b></p> <p>The shortest way from your Inbox to SpamCop is by forwarding your spam to SpamCop for analysis.</p>	<p>Reporting spam via SpamCop's Web interface is a great way of fighting it.</p> <p>Report spam here: <a href="http://www.spamcop.net/anonsignup.shtml">http://www.spamcop.net/anonsignup.shtml</a></p> <p>But the constant view-message-source — copy — open-SpamCop-page — paste — submit cycle can get time consuming and tedious if you get lots of spam. That's why I prefer to submit my spam via email.</p> <p>To submit spam to SpamCop via email, you first need to find out your personal submission email address. Every registered user has one, and it is displayed on the SpamCop home page, right below the welcome message.</p> <p>Now forward unrequested, unwanted emails to this address to have it parsed by SpamCop.</p> <p>It is important that you forward the message as an attachment and not inline. One of the big advantages of submitting spam via email is that you can insert multiple messages at once: just forward them in one email.</p> <p>Once SpamCop has processed the spam, it will send a mail back to you containing the URL you can use to report the spammer.</p>

<p><b>Use a Good Anti-Spam Program</b></p> <p>Achieve a near spam-free email account by employing one of the great anti-spam tools that filter junk mail using all kinds of clever strategies.</p>	<p>Spam isn't that bad — if I never see it.</p> <p>This is the aim of anti-spam tools. They promise to clean your email account of spam before you download the new messages in your favorite email program. And quite often, they do succeed.</p> <p>The best anti-spam tools work great out of the box but also allow a good amount of flexibility and configuration. They are easy to set up and efficient at pointing and deleting unwanted, unsolicited mail.</p> <p>Choose your favorites:</p> <ul style="list-style-type: none"> <li>• Top Anti-Spam Tools for Windows</li> <li>• Top Free Anti-Spam Tools for Windows</li> <li>• Top Anti-Spam Plugins for Outlook</li> <li>• All Anti-Spam Tools for Windows</li> <li>• All Anti-Spam Tools for the Mac</li> <li>• All Anti-Spam Tools for Linux/Unix/BSD</li> <li>• All Anti-Spam Services</li> <li>• Bayesian Spam Filtering Tools and Services</li> </ul>
<p><b>Spam is Named After Monty Python's Spam Skit</b></p> <p>Why unsolicited email is called spam. And spam.</p>	<p>Have you ever wondered what unsolicited email messages have to do with canned meat?</p> <p><b>Etymology of Spam: Canned Meat and Vikings</b></p> <p>Have you ever seen episode 25 of Monty Python's Flying Circus? In the Spam skit, customers can order only dishes containing SPAM, SPAM, and SPAM.</p> <p>Similarly, you can't have email without spam. And spam.</p>
<p><b>Choose ISPs by Their Spam Policy</b></p> <p>Don't support spam-friendly internet service providers.</p>	<p>If I tell my computer dealer there are other shops where I can get this-and-that with better service for a lower price, I usually get what I wanted. The same holds true for ISPs and spam.</p> <p>If you choose an ISP,</p> <ul style="list-style-type: none"> <li>• make sure they not only act aggressively against their own spamming customers and</li> <li>• possibly filter incoming spam, but also</li> <li>• prevent harvesting of their network and</li> <li>• don't host spamvertised Web sites.</li> </ul>
<p><b>Know What a LART Is</b></p> <p>A LART is a luser attitude readjustment tool. Find out what this is.</p>	<p>If you heard serious anti-spammers talk, you may have heard them demand: "Lart that spammer!" Sounds pretty terrifying, and in a way it is.</p> <p>LART stands for <b>Luser Attitude Readjustment Tool</b>, with a luser of course being somebody who is at the same time a user and a loser.</p> <p>In the context of spam, applying LART on a user (a spammer in this case) usually means exercising the ISP's acceptable usage agreement.</p> <p>Most ISPs do not allow their users to send unsolicited bulk email. Violating that policy usually means discontinuation of service, and that's what larting a user means.</p>

<p><b>Use Bayesian Spam Filtering to Get Rid of Junk Email</b></p> <p>Get rid of spam reliably, precisely and effortlessly with statistical means.</p>	<p>Of all the spam filtering techniques, Bayesian spam filtering is the most promising. By analyzing messages that you have classified as spam, Bayesian junk mail filters can calculate the probability of new mail being spam.</p> <p>Bayesian statistics-based spam filters and filters using other smart adaptive artificial intelligence techniques promise to be the most effective. Bayesian spam filters calculate the probability of a message being spam based on its contents. They learn from spam and from good mail, resulting in a very robust and efficient anti-spam approach that returns hardly any false positives.</p> <p>Since Bayesian spam filters not only take spam into account but also look at all the good mail, they can get a pretty good idea what is characteristic of spam, and since they learn with every message, Bayesian spam filters adapt to the latest spammer tricks automatically.</p> <p>To make use of Bayesian spam filtering</p> <ul style="list-style-type: none"> <li>choose from the growing number of email clients, anti-spam tools and general filters implementing Bayesian spam filtering.</li> </ul> <table border="1" data-bbox="716 440 1549 698"> <thead> <tr> <th data-bbox="716 440 905 483">Email Client</th> <th data-bbox="905 440 1549 483">SPAM Tool</th> </tr> </thead> <tbody> <tr> <td data-bbox="716 483 905 698">Outlook, Eudora, Mozilla, Netscape, and Thunderbird</td> <td data-bbox="905 483 1549 698">Cloudmark, Email Magician, eXpurgate, Popfile, SpamPal, Spamihilator, K9-Spam Filter, Spam Bully, Spamoto, Spam-Experts Desktop, Cactus Spam Filter, many more ...</td> </tr> </tbody> </table>	Email Client	SPAM Tool	Outlook, Eudora, Mozilla, Netscape, and Thunderbird	Cloudmark, Email Magician, eXpurgate, Popfile, SpamPal, Spamihilator, K9-Spam Filter, Spam Bully, Spamoto, Spam-Experts Desktop, Cactus Spam Filter, many more ...
Email Client	SPAM Tool				
Outlook, Eudora, Mozilla, Netscape, and Thunderbird	Cloudmark, Email Magician, eXpurgate, Popfile, SpamPal, Spamihilator, K9-Spam Filter, Spam Bully, Spamoto, Spam-Experts Desktop, Cactus Spam Filter, many more ...				
<p><b>Whether or Not to Unsubscribe from Spam</b></p> <p>If junk mail that lands in your email inbox contains unsubscription instructions, does it make sense to follow them?</p>	<p>Spam is best filtered away, never to be seen.</p> <p>Once in a while, junk email may make it to your email inbox, though, and — lo and behold — it contains an "unsubscribe" link. Or is it a purported "unsubscribe" link?</p> <p><b>A Wasted Effort?</b></p> <p>Generally, the content of spam is not to be believed, and that applies to all promises to take you off the list as well. From that avenue, unsubscribing from spam is wasted effort better to be spared elsewhere.</p> <p><b>What Could Happen if You "Unsubscribe"?</b></p> <p>Then, of course, you're already getting the spam. If you follow the unsubscription instructions that are easy to follow, you can be taken off one spammer's list — or at least you're not off much worse. (Take care not to be tricked into giving away any data other than your email address.)</p> <p><b>Be Nice to Newsletters You Don't Like (Any Longer)</b></p> <p>Finally, there's the chance that what you not think is spam looked like a nice newsletter to sign up for seven years ago. If you use the unsubscription method offered instead of reporting the email as junk, you spare the publisher and your email provider a lot of hassle, and you make spam filtering much more effective.</p>				
<p><b>Do Not Threaten Violence to Spammers</b></p> <p>Is fighting violence with more severe violence a good idea?</p>	<p>Spam is bad, and spamming is bad, but that does not automatically make spammers bad people. It's natural to get emotional about receiving unwanted email, but this should not make you threaten violence to spammers.</p> <p>Sometimes,</p> <ul style="list-style-type: none"> <li>explanation and education will do the trick,</li> <li>but if you have to resort to threatening,</li> <li>do it with legal means (by means of the law and sanctions enacted by society, such as a refusal to accept any mail from people and organizations affiliated with spammers).</li> </ul>				

<p><b>Feed Hotmail Into SpamCop</b></p> <p>Trace, analyze and report the spam you receive at Hotmail with ease, and with the help of SpamCop.</p>	<p>SpamCop makes reporting spam correctly a snap. But how can you use it for unsolicited messages you receive at your Hotmail account? To make mail digestible for SpamCop, it needs to come in its rawest form: no HTML, full headers. Windows Live Hotmail has an efficient way to let you see exactly that.</p> <p><b>Feed Windows Live Hotmail Into SpamCop</b></p> <p>To process and report spam you have received at Windows Live Hotmail with SpamCop:</p> <ul style="list-style-type: none"> <li>• Make sure you use Windows Live Hotmail (not Windows Live Hotmail Classic).</li> <li>• Open the junk email's source.</li> <li>• Highlight all of the message's source which opens in a new window.</li> <li>• Click in the frame containing the source and hit <i>Ctrl-A</i> (Windows, Linux) or <i>Command-A</i> (Mac).</li> <li>• Press <i>Ctrl-C</i> (Windows, Linux) or <i>Command-C</i> (Mac) to copy the source.</li> <li>• Paste it into your SpamCop account, analyze and complain about it.</li> </ul>
<p><b>How to Disguise Your Email Address in Newsgroups, Forums, Blog Comment</b></p> <p>Make it more difficult for spammers to get your address by obfuscating it when you use it in newsgroups, forums and the like.</p>	<p>Spammers use special programs that extract email addresses from chat rooms, web sites — forums and comment sections of blogs in particular — and Usenet postings.</p> <p><b>Disguise Your Email Address in Newsgroups, Forums, Blog Comments, Chat</b></p> <p>To avoid ending on a spammer's mailing list when you post to a web forum or a newsgroup, you can</p> <ul style="list-style-type: none"> <li>• disguise your email address by inserting something obvious into it.</li> </ul> <p>If my email address is me@example.com, I can modify it to read me@EXAdelete_thisMPLE.com, for example. I will not get spam at that email address since all messages to it will bounce, but people who want to send me an email can still do so after they remove "delete_this" from the address.</p> <p>Obscuring your email address does make sending mail a bit more difficult. But this is not always a disadvantage.</p> <p><b>Automatic Email Address Obfuscation</b></p> <p>Email address encoding tools take the obfuscation a step further. While primarily designed for use on web sites, you can also use addresses encoded with such tools on web forums or web-based usenet, for example.</p> <p>To prevent your email address from being picked up by spammers from your web site, you should obfuscate it in some way. You can do that by hand, or employ one of the tools dedicated to it, which will usually do a better job more comfortably.</p>
<p><b>Filter Spam Using ISP-Supplied Junk Mail Headers</b></p> <p>Maybe your Internet Service Provider runs a spam filter that changes messages subtly if it believes they are junk. Here's how to make use of this simple yet effective line of spam defense.</p>	<p>You don't like spam, and most probably your Internet Service Provider does not either. Many run <a href="#">SpamAssassin</a> or a similar spam filter on the mail server.</p> <p>These spam filters are not perfect, but they can be a great help with the daily junk mail avalanche. Subtly, they add <u>headers</u> to the emails going through them, indicating whether they believe a message to be spam.</p> <p>If your email client can filter on arbitrary header lines (unfortunately, <a href="#">Outlook Express</a> for example does not), you can use these ISP-supplied headers for easy yet effective spam filtering.</p> <p>To filter spam using ISP-supplied junk mail headers:</p> <ul style="list-style-type: none"> <li>• Set up a rule in your email client that</li> <li>• moves incoming messages to the "Spam" folder</li> <li>• if the email header includes "X-Spam-Status: Yes".</li> </ul>

<p><b>How Long, Complicated Email Addresses Beat Spammers</b></p> <p>Spam will, eventually, make it to any mailbox. Any? Here's how to make it hard for spammers to guess your address.</p>	<p>If you post your email address to the net, chances are it will fall in the hands of spammers. But even if you never expose your address to a place where spammers may collect it, you will probably get spam.</p> <p>That's because spammers apply another technique to find email addresses, too. They simply guess. Given a domain name, spamware will send mails to all kinds of (likely) user names at that address, from aaaronb@ to zzziddyw@.</p> <p>You can escape this attack of brute force like you can (try to) escape somebody guessing for your password. Try to make your address as difficult to guess as possible when selecting your user name.</p> <p><b><u>Long, Complicated Email Addresses Beat Spammers</u></b></p> <p>To beat spammers, use a</p> <ul style="list-style-type: none"> <li>• long email address</li> <li>• consisting of more than one word</li> <li>• and, preferably, word segments as well as</li> <li>• numbers and</li> <li>• an underscore.</li> </ul> <p>Of course, there's no point in constructing an email address that is impossible to guess for you, too, on odyssey to spell over the phone and hard to type for your friends.</p>
<p><b>How to Report Spam with SpamCop</b></p> <p>Complain about spam the right way easily with SpamCop, which does all the analyzing for you and generates a perfect complaint email, too.</p> <p>B</p>	<p>There are strategies to avoid unsolicited email, and you can filter it away or ignore it.</p> <p><b>Why Reporting Spam Makes Sense</b></p> <p>One of the best things you can do about spam, however, is to receive it and complain about it. Spammers will consequently lose their Internet access and pay for their breaking an ISP's acceptable use policy.</p> <p>Identifying the right people to complain to about spam and writing complaints efficiently unfortunately is not a trivial matter, however, and it takes a lot of time.</p> <p>This is where SpamCop can help. It analyzes your unsolicited email messages and sends sensible complaints to the right authorities on your behalf.</p> <p><b>Report Spam with SpamCop</b></p> <p>To submit a correct and efficient spam report using SpamCop:</p> <ul style="list-style-type: none"> <li>• Open the source of the junk email in your email program.</li> <li>• Highlight the full source and press <i>Ctrl-C</i> (Windows), <i>Command-C</i> (Mac) or <i>Alt-C</i> (Unix) to copy.</li> <li>• Paste the source of the spam you received in the SpamCop input field.</li> <li>• Press <i>Process Spam</i>.</li> <li>• Click <i>Send Spam Report(s) Now</i>. <ul style="list-style-type: none"> <li>○ It's usually best not to change anything about the complaints unless you have a good reason to exclude or include a specific email address not preselected.</li> </ul> </li> </ul>