



**This ebook is brought to you buy**

Buy-Ebook.com

[www.Buy-Ebook.com](http://www.Buy-Ebook.com)

**Want to make money with this ebook?  
Become an authorized distributor today by [clicking here!](#)**


Liz Tomey  
2005 [TomeyMarketing.com](http://TomeyMarketing.com)

#### Limits of Liability/Disclaimer Of Warranty

The publisher and author of this book and all products related to this book have used their best efforts in creating this product. Neither the publisher nor the authors make any representation of warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this program. They disclaim any warranties that are either expressed and/or implied merchantability, or fitness for any particular purpose. The author and the publisher shall in no event be held liable for any loss or other damages, including but not limited to special, incidental, consequential, or other damages. The advice of a competent legal, tax, accounting or other professional should be sought. You do not have the right to give this ebook away, include it in any membership site, or offer it as a bonus! You may not sell this ebook unless granted permission or have become one of our authorized affiliates. If you are in violation of Our copyright or our terms and services, we will take the actions we need to take against you.

**To make sure you have the up to date copy of this ebook, please [click here.](#)**

## The SPAM Files

	<p><a href="http://MarketingForREALPeople.com">MarketingForREALPeople.com</a> was built out of disgust for the Internet marketing market. After months of buying, reading, and searching, I decided to really start dissecting everything I bought and read.</p> <p><b><i>The outcome?</i></b></p> <p>A site made for REAL people just like you. Have you spent hours and hours reading and searching for that perfect product that's going to make you a killing? Let's not even talk about the amount of money you have probably spent. That all stops right</p>
---	--

<b>Welcome to the World of Spam! .....</b>	<b>Pg. 3</b>
<b>Here's What SPAM is? .....</b>	<b>Pg. 4</b>
<b>The Tricks of the Trade – How They Get Your Information .....</b>	<b>Pg. 6</b>
<b>SPAM is not JUST Annoying .....</b>	<b>Pg. 11</b>
<b>Danger Zone .....</b>	<b>Pg. 12</b>
<b>Do SOMETHING About IT! .....</b>	<b>Pg. 13</b>
<b>Even More Things You Can Do About Your SPAM Problem .....</b>	<b>Pg. 17</b>
<b>A SPAM Free Email Service? .....</b>	<b>Pg. 21</b>
<b>Don't Let Your Password Be Naked! Clothe It With Encryption .....</b>	<b>Pg. 23</b>
<b>Pass the Beggars By Online .....</b>	<b>Pg. 24</b>
<b>You're Going TO Get SPAMMED!!! .....</b>	<b>Pg. 25</b>
<b>SPAM FILES .....</b>	<b>Pg. 27</b>
<b>Need More Info? .....</b>	<b>Pg. 29</b>

## **Welcome to the World of Spam!**

Computers have become an integral part of life for nearly everyone in the world. Ever since the induction of the Internet, they have become very commonplace in most businesses and homes. Most people cannot even imagine their lives without their computers.

They are used to run businesses, keep track of inventory, gather information, and to communicate with people from great distances.

Naturally one of the most popular reasons that people use the Internet is to send emails to others. It is a free and easy way to talk to people that live far away. You can use emails to send letters, data files, and pictures.

Everybody likes to get an email from his or her friends and family. However, emails have also become a popular tool that is used to advertise products and services.

As much as we like to receive emails from those that we enjoy hearing from, nobody likes to receive emails from people we've never heard of. These emails are called SPAM.

We know how annoying it can be to receive SPAM in your email everyday. We decided that it was time to write a comprehensive guide on what you can do to stop these types of emails from getting into your account.

Of course we can't prevent companies from trying to send them, but we can arm you better against them.

This ebook was written so that we could provide you with your comprehensive guide to fighting against, and hopefully someday; completely stopping unwanted emails from reaching your inbox.

## Here's What SPAM is?

The best place to begin would be to explain to you exactly what SPAM mail is. SPAM is basically just unsolicited commercial emails that companies send to your inbox.

There are a lot of reasons why these companies get your email address. You may have signed up for a newsletter or promotions with one of them, or you may have ordered a product or service that requires registration from a website first.

It is common for companies to share their mailing lists with their affiliate companies. It's one of the benefits to having affiliations. The only problem is that most companies hide this knowledge in their "terms and agreements" of their websites. They count on the fact that most people do not read all the way through them. Of course since it is mentioned somewhere in their website, it is perfectly legal.

The average person can expect to receive anywhere from ten to twenty SPAM emails a day in their inbox; depending on how many promos and registrations they fill out. Once a person accepts or opens an unsolicited email, they become plagued by receiving six more in its place. It is a vicious cycle.

As the Internet has reached its peak popularity during the past couple of years, so have companies followed suit and expanded their abilities to advertise. The biggest problem is that they don't know when to stop advertising. The best place to begin with this manual is to give you a list of some of the things that you may do that will leave your inbox vulnerable to receiving SPAM.

- **Filling out a registration for an online newsletter is a common way for companies to use your inbox to advertise.**
- **Registering your inbox for promos and contests.**
- **When installing new software it is common to register your email address for updates, but it is also leaving yourself open to SPAM.**

## The SPAM Files

- **Signing up for just about anything online is leaving yourself open to receiving SPAM.**

One Common factor in all of these things listed is that you have to volunteer your email address to a company before it can be used. Of course, there are ways for a company to get your email address without you having to give it to them directly.

## **The Tricks of the Trade – How They Get Your Information**

A company can give your email address to an affiliate of theirs when you give it to that company, but that is not the only way that a company can get your email address. These days, companies are getting smarter in their efforts to attain email addresses. Here are some of the ways that companies are getting a hold on your inbox.

### **Personal Homepages**

Just about everyone has a homepage of their own these days. Almost every Internet service provider (ISP) offers you a place to put up your own website. The problem behind this is that when you do put up your website, you often feel obligated to leave your contact information.

This is not a very good idea if you are looking to avoid SPAM because you have just advertised your email address. A resourceful person will take down your information so that they can SPAM you later.

A lot of people don't think that they can receive SPAM simply from putting out their contact information, but it is the easiest way to do it. Spammers can easily gather all of your information by using what is called "Harvesting Software".

Harvesting software is basically a program that searches the Internet for the @ symbol. In searching for it, they recognize that this is likely an email address and therefore it leaves you open to receive their spam. Most of the time, spammers are unaware if the email address is even active or used at all. That is why they can put out so many of them.

By harvesting as many of the addresses that use the @ symbol, spammers are basically guessing that at least 50,000 emails they send out of 1,000,000 of them will be viable. In most cases, regular people like you prove them right by responding to them.

Once you reply to one of the spam that you receive, you have announced to them that they can continue to send you email. You should know that they will often report your email address to other companies and their affiliates which will only lead to your receiving even more spam.

### **Registration Forms**

## The SPAM Files

Whenever you are interested in signing up for a service online, you would serve yourself better not to leave your email address unless you are certain that you want to receive news and product announcements from that company.

Nearly all registration forms that you fill out can lead to spam. That is why these companies ask you to fill out registration forms. Some companies leave you with the option of receiving emails and notices from them. You should always read the fine print of a registration form before you submit it.

There is usually a box that you can check if you do not wish to receive emails from the company or its affiliates. If you do not wish to receive them, you should be certain to check that box. If that box doesn't exist, then you may want to forget the registration all together, just to be sure.

Of course, it is common for some companies to place the option on receiving emails or not and still send you emails. That is why you should always check the privacy policy of the company first. It is the law that all companies let you know whether or not they share your information with others. It is also common for people to ignore the privacy policy information.

That is why you should always read through it.

It does take some extra time on your part to go through these policies, but you can save yourself the effort of having to go through and delete SPAM, which is more annoying. By not going through the privacy policy, you are playing roulette with your inbox.



**Brand New** Internet Advertising Has Changed Forever!  
**Advertising Methods**  
**To Explode**  
**YOUR**  
**Profits!!**

**VIRAL**  
**EbookAds.com**

**Your ad ALL OVER the Internet**

**Think about that for a minute. Do you see the potential of VIRAL marketing? Now go put it to work for you!**  
[Click Here!](#)

This registration SPAM also applies when you are registering a new piece of software. After you have installed the software, there is often the task of

### The SPAM Files

registering. Many of the companies tell you that registering it is so that you can be informed of any product upgrades for that software. But you should know that they are also used to send you every other notice about their company as well. If you don't want to receive this type of information, you have to refuse the registration process.

## **Cookies and Temporary Internet Files**

Spammers use software programs called spiders to access and harvest your email address. These spiders basically just wander around the Internet and into active browsers searching for your email information. To be more specific, they are looking for the @ symbol so that they can attach themselves to email addresses.

These spiders are very intelligent, but not intelligent enough to know the difference between a legitimate email address and a simulated address. They grab everything and harvest the information to their own database. They can also sometimes grab information from your browser that is not an active or viable email address. These come in the form of cookies and temporary Internet files.

If you don't know what cookies and temporary Internet files are, they are they are the record that your computer takes of your online surfing. It is how your computer is able to bring up recently typed in information and quick launching any sites that you want to revisit.

The reason the spiders harvest your cookies and temporary internet files is because the cookies are saved in a manner that resembles an email address. Cookies look like this: [MBrown@anywhere.com](mailto:MBrown@anywhere.com) they usually take on the registered name that the computer is registered to and doesn't leave a website's name.

You could gather up to 50 cookies a day depending on how many websites that you visit during the day. Since the spiders don't know the difference between real email addresses and cookies, you would do better to clean out your cookies and temporary Internet files at least twice a week; more if you surf a lot. Here is how to do it from windows.

You can begin by double clicking programs, then accessories, then system tools, and then click disk clean up. Click okay when that box comes in and you can

delete your old files and cookies. You can also remove your cookies and temporary Internet files by:



## The SPAM Files

*Right clicking start, click settings, then control panel. Go into your Internet options icon. In there you can follow the instructions for you to clean up your computer by deleting both cookies and temporary Internet files.*

It is a relatively easy thing to do once you get used to it. In doing this, you are getting rid of the extra files on your computer that these spiders are looking for. It is just an extra precaution that is good to take.

## **Contest Entries**

An alluring way for companies to get your email information is to post contests for things that you would have an interest in winning. Of course in order to enter, you must provide your email information so that they can notify you if you win.

What they don't tell you is that you are also leaving yourself open to spam from them. Most people know that this is the plan, and many think that this is worth it, but if you don't, you should think twice before signing on the line.

This also applies to gift offers and subscriptions. It can be a real bother to go through all of the effort it takes to sign yourself up for a contest that has been set up specifically to harvest your email address.

Before signing on for any contest, you should always check the company that is offering it. Some of these contests are legitimate, and some of them are set up specifically to get your email address. It's a really tricky business. The prize may not always be worth the amount of spam you receive.

## **Remembered Email Information**

A common practice among the more sophisticated spam artists, is to get a good grip on those internet users that have a habit of saving their sign in information to their email addresses. It is very rare, but some people do have the knowledge to pick up your login information.

### The SPAM Files

If you can avoid it, you should try not to save your information like that. It might save you seconds from putting in all of your information manually, but it also leaves you vulnerable to getting snooped.

You have to understand that some spammers get together with hackers and then you have a real problem. That is when their spam can be dangerous to your computer.

When spammers do this, they can sometimes be detrimental to your computer's health to even open the email because it could be an automatic virus that is in your inbox instead of just an annoying ad.

## **Public Posting**

When signing up for one of the many free email addresses that are out there, many people decides to add themselves to the public profile list that the email provider offers. Generally, you leave your basic information and screen name. However, what you rarely notice is that you also leave your contact information as well.

Someone that has little else to do with their time can easily search through public profiles and get your email address at will. The common user will take this information in order to have a chat with someone that shares their interest, but a person that wishes to send you spam can also contact you whenever they want.

In general, you will want to avoid filling out any forms that require you to give out personal information like that. You should always read the company's privacy policy as well. I know they can be a bit long winded, but true spammers want it that way because they depend on your not reading it. This is how they sneak in the fact that they plan on sharing your information with other companies, if in fact they do.

## **SPAM is not JUST Annoying**

## The SPAM Files

Spam can be a lot more damaging than you might think. Obviously, they are the most annoying things that you can receive through your inbox, but it goes deeper than that. If you are like the millions of other internet email users, you know that sending and receiving email is a free service that comes with your internet service.

Internet service providers are great for providing you with a way to send letters to your friends and family while saving you the cost of postage and envelopes. You can even send cards for free with an email address. But don't let the free service make you think that you don't actually have to pay for it. Let me explain.

Internet service providers and web hosts do not get their email services for free. They have to pay for something that we do not have to pay for as consumers. They have to pay for bandwidth. That might not mean much to you, but for these companies, it means that they are forced to produce mass emails, and this means that their costs increase as well.

It may not seem to be a matter for the mere consumer, but let me tell you that this does affect you; here is how:

Since they are forced to send mass emails, which in turn raise their costs for service, you as the receiver are forced to pay more money for your internet service. This in a way helps ISP's to reduce their overhead costs.

Some of the cheaper ISPs like Net Zero help to cut their costs down by charging outside companies money to SPAM and add those annoying pop-ups to your homepages. Since the advertisers are paying for their pop-ups, you get a break on the cost of using them as an ISP.

Other popular companies use affiliations to assist them with keeping their costs down, eventually leaving the consumer with a pretty good rate. I'd prefer to use an ISP that simply goes for the search engine affiliation as they have much better pop-up prevention on their side, and they actually provide you with a service.

## **Danger Zone**

### The SPAM Files

These are not the only problems that accompany SPAM. They can also be used by some spammers to put viruses, worms and Trojans into your computer. I'm not saying that every company uses SPAM to input viruses, but many of them do.

What you have to know is that not all viruses are meant to shut you down or crash your computer. Some are more to spy on you when you are online. They are called spyware, and adware. This is how some of these companies force you to go into their websites every time you go into your search engine.

This is a very popular way for spammers to get into your daily routine. A lot of these types of spammers' programs will attach themselves to your computer's operating system in a way that prevents you from removing them because in getting rid of these programs, you will ruin your computer's ability to function properly. It is an ingenious way of forcing their products and/or services on you.

Many times when this happens, you are forced to have to completely reboot your computer and set it up again from scratch, which is why it is always good to have a backup of all of your information on disk, at least for the items that you cannot afford to lose. A good resource to help you with this can be found at [http://www.viralbuzz.com/stop\\_email\\_spam.html](http://www.viralbuzz.com/stop_email_spam.html)

The graphic is a rectangular advertisement with a yellow background and a black border. At the top, the text "TomeyMarketing.com" is written in a black, typewriter-style font. Below it, the slogan "Marketing for REAL people!" is written in a smaller, similar font. To the right of the text is a cartoon illustration of a man wearing a hat and glasses, reading a newspaper. Below the top section, there is a white rectangular box containing the text: "Visit [TomeyMarketing.com](http://TomeyMarketing.com) today for **unique advertising services** that get results, and incredible products that will help you **build your business!**" The words "unique advertising services" and "build your business!" are in red, while the rest of the text is in black.

**Do SOMETHING About IT!**

## The SPAM Files

Dealing with the after effect of SPAM does not have to be like pulling teeth. It can be easier than that. Of course it helps to know some of the easiest ways to keep SPAM from ruining your online experience.

Sometimes you can receive so much SPAM a day that you could spend more of your time deleting these annoyances than responding to your legitimate emails. By the time you have finished messing around with your emails, you could be far too frustrated to be bothered with anything else. However, there are some things that you can do to make your online experience a little bit easier. There is some ways to keep spam from ruining your day. Here is a list of some of those things.

## **Email Filters**

Filters are a very effective way of managing or getting rid of unwanted emails, but sometimes they can work too good. While they can work very hard to keep your inbox from receiving spam, they can also prevent you getting a lot of your wanted emails as well.

Some of the worst filter based systems for blocking spam are provided by your very own ISP. This can be a big problem because these types of filters do not let you control which emails that you can let through.

Basically, these filters search for common key words and phrases like Guaranteed, free, and so on. Once these systems pick up on those key words, it will automatically prevent those senders from sending you emails again. That can be very annoying if such a keyword is used by a friend or family member to describe the reason they are emailing you in the first place.

If you would prefer to use this type of method for SPAM prevention, let me suggest that you get the type of filter that allows YOU to control what content is allowed and what should be deleted. Here is a link on this very subject:

<http://www.spamarrest.com>

## **Paid Email**

Forcing people to pay for every email they send would certainly put an end to spam, but it would likely put an end to anybody sending emails as well. The entire reason why most of use emails is because it is a free service. That is the reason that it is so popular in the first place.

## The SPAM Files

Spammers would find that paying for the right to harass you through your inbox would definitely be a good reason to stop bothering. However, it would also prevent the average user from sending emails as well.

Of course, it is inevitable that even if an Internet company decided to charge you one half of one cent to send an email, eventually spammers would find a way to get around that as well. It is the very technology. As honest people continuously search for their online privacy; as lawmen continue to find new ways to prevent spam; so do spammers continuously find methods of beating the system.

Basically in most of our efforts to prevent these spammers, we are accomplishing one indefinite feat. We are making these people smarter. They get smarter with every effort that we make to make their irritating use of emails illegal. It is a very big waste of time.

## **National No-Spam Directories**

These work basically the same as the National tele-marketing laws do. There is no such thing that works for the Internet yet, but this is the way it would basically be if there was such a law in existence.

You would have to call a special number or go to a web link, and place your email address in a no call area. This would mean that if any company wanted to send you spam, it would be completely illegal, and they would be susceptible to criminal charges.

At this moment in time, this type of law does not currently exist. It is a difficult law to pass since it basically infringes on a great many rights of the spammers. Yes it does stink that they have rights also. If you would like more information on spam laws check out this link. <http://www.spamlaws.com>

## **Complaining to Spammer's ISP**

Complaining to a spammer's ISP is another route that you might take, but it utterly useless. As there are no laws as of yet to prevent them from sending you spam, there is little that you do about receiving them. At least as far as it concerns the ISP.

These days spammers are smarter than your average surfer. All ISPs can really do is threaten to shut them down. That is not a permanent solution because

## The SPAM Files

spammers just learn to use different methods to get their emails out. They can do any of the following:

- **Change their e-mail's return address.**
- **Change their title and/or user name**
- **Use multiple credit cards**
- **Use various forms of different identification**

Basically, if you learned anything from this area, it must have been that complaining is really a waste of time because spammers have far too many ideas on how to avoid ISP interference for the ISPs to have any affect at all. In the end, the best things that you can do for yourself is to try and follow some of the easy techniques listed below for some pretty good tips on avoiding annoying spam in your inbox.

## **Challenge Response Filtering**

This is a really cool and easy method to use for dealing with spam. What this does, is forces anybody that you have not already cleared to email you to fill out a short form or click a special link in order for their email to go through.

It also lets you create a safe list. This is just a list of people that can send you emails without making them fill out the form first. Again the link for this can be found at <http://www.spamarrest.com>

The purpose of using this type of system for keeping SPAM away is that it is pretty rare for one of these companies to take all of that time just to send one person an email. Of course there is always the chance that some spammer that is in desperate need for a life might just do that.

On the off chance that one of the spammers does manage to take the time to fill out this report, you can simply get rid of them by taking them off of your safe list or just deleting and blocking them permanently from your computer.

Some of the better washers will hold many of the challenged emails in a pending folder and let you decide yourself which ones to clear through to your inbox. All this means is for those people that take the time to fill out the form or click on the link, they are still sent to a "maybe" box. This lets you decide manually which to

## The SPAM Files

keep and which emails to get rid of and block. In a way, it's one of the best methods out there right now.

### **Mail Washers**

This method is an extremely effective way of dealing with spam. What it does is it lets you check and/or scan your emails before they even reach your inbox. This is a rather cool way to deal with unwanted spam.

If you can combine this method with a challenge response system, you can ensure that your inbox remains 100% free of spam and email viruses. Really, isn't that why you are reading this guide in the first place?



## Even More Things You Can Do About Your SPAM Problem

For all of the things that you can try to do that do not work for getting rid of spam, there are in fact, some that do work. The best thing to try and remember is that you will never really be able to completely avoid receiving spam.

After all things are said and done not everyone wants to spend all of the extra money that it takes in order to get rid of spam. Not to mention; not everyone can afford it either. If this sounds like you, there are a few things that you can do that will not cost you anything except a few moments of your time. In the end, isn't it worth it?

Here are a few things you can do that actually work!

### Ignore Them

You should never open an unsolicited email that you receive in your inbox. You have to understand that spammers are really just playing a numbers game. They simply send out like a million emails and hope that at least a third of them stick. It's sad but it's true.

 <p><b>GuruMarketing Articles.com</b></p>	<p>Articles aren't just for the Gurus anymore! Anyone can promote their business with articles. They're easy to write and can get you A LOT of publicity! Visit:</p>
<p><a href="http://www.gurumarketingarticles.com/">http://www.gurumarketingarticles.com/</a></p>	

### The SPAM Files

See, a spammer's goal is to simply gather as many email addresses as they can get their hands on. They don't even know if any of the addresses are even active; they simply hope that they are. It is when you answer them that they know whether or not it is an active account that is checked often.

The people that send spam are not stupid, they know that it is highly annoying for you to get their emails, that is why they send out so many of them. It is simple odds; for every person that ignores their emails, there is one that opens and answers them. With odds like that, can you really blame them for continuing to send spam?

## **Do NOT Click On the Unsubscribe Links**

This kind of goes along with ignoring the SPAM emails. Often spammers will approach you in a way that let's you think that they are your friends. They will put certain things in your subject line like these:

- **FROM: Paulina, SUBJECT: "remember me?"**
- **SUBJECT: hi**
- **SUBJECT: guess what?**
- **SUBJECT: (none)**

You get the picture from those. Many spammers will leave names and casual greetings so that you believe that you are getting a friendly email from a friend. Actually, that is a very useful method. I know plenty of people who have been caught by that one. Especially if the spammers use a name and that name is the same as a contact.

Of course, once you open these emails, you realize very quickly that they are not from your friends, but advertisements. It is natural for you to want to click on the link at the bottom of the email that promises that you can be taken off of their email list, but do not think for a second that this is what happens.

When you click on the "click here if you wish to stop receiving these emails" link, the spammers simply change the name that sends it to you. You will still receive the offensive material it will just be under a different name and subject text.

### The SPAM Files

Hopefully you will now know that it is a waste of time for you to try to and get your address off their list. All you have proven is that you are indeed opening and reading them. So you have set yourself up as fair game.

## **Use Various Email Addresses**

Since it is unavoidable to receive spam, you may want to set up a “dummy” email address. You would use this address when you register for newsletters, order products, enter contests, and register your new software.

You would like to avoid using your primary email address, or the email address that you receive from your ISP for things like that. This is the email that you would give your contacts or “safe people”.

Naturally you will still receive some spam in your primary address, but at least not all of your time will be spent dealing with them. You can check your dummy address about once a week, or more if you really feel it is necessary.

## **Don't Post Your Address**

When you are on the Internet or using a homepage of your own, you will also want to avoid posting your email address in your “contact me” section.

Since spammers scan through different homepages and look for the @ symbol, you would serve yourself better to write your email address with the word “at” instead. That makes it a bit more difficult for spammers to find your email address because they use special software that searches for the symbol, and not just the words. It won't stop it completely but it will help.

## **Do Not Purchase from Spam**

The biggest reason why spam is out there is because certain people have some sort of product or service that they are trying to sell. The absolute worst thing that you could do is buy something from them. Obviously, we can't make everyone refuse to purchase his or her wares, but you can at least do your part.

Just imagine how perfect the world would be if everyone gathered together to refuse to buy things that were offered in an unsolicited email. Spammers would

## The SPAM Files

be out of business the moment that they realized that they weren't getting anywhere.

### **Beware of Free Trial Software**

One of the best reasons for going online is to download software and games that make surfing on your computer more fun. These days you can go to almost any website and find free software to try, and download. This can be very rewarding and entertaining at times, but there is a down side to doing this as well.

For every legitimate download, there are plenty that are designed to get your personal information, which will eventually lead you to more spam. This is particularly popular from free trial software as well as free software.

Spammers use this method in a similar manner as they would use a gift promotion and contest sign in. You see, they will let you have their software under the strict regulation that you leave yourself open to receiving updates and notifications about their products. Many people agree to this because they are getting something out of the deal besides the software.

That is one of the most beneficial ways for spammers to get you on their hook. Usually you can check their privacy policy or terms of agreement policies before you install it. You should ensure that you check these before agreeing to sign up. If not just for the spam you may receive, then for viruses and worms.

You should always check to see who their affiliates are as well before you download from a website, as sometimes you have to deal with their spam as well.

## **A SPAM Free Email Service?**

Some free email service providers have some pretty good blockers' services to accommodate you a bit better. My favorite is the free version of Hotmail provided by msn. Don't get me wrong, plenty of the free email service providers are trying to get on top of the spam epidemic.

With this free email service, you can set up your account to keep only your personal contacts in your email inbox. The rest of the emails automatically go to a junk mail folder that you can check out at your own time. If you don't check them within seven days, they are automatically deleted.

The msn messenger, which is used to send instant messages to people, can be checked by right clicking the messenger icon. If you have received email from your contacts it will show you and you can go directly to your inbox by left clicking the messages text. If you have junk mail it doesn't show up. It is perfect.

Of course your junk mail section can still receive SPAM, but now it is at your own leisure that you check them out. Yahoo has a similar system, but with the Yahoo messenger instead. This method is not fool proof, but it is still pretty good if you don't want to spend the extra money for new software.

Free email providers like Yahoo and MSN are very good providers because they are very intent on keeping spam out of your inbox. They are just as interested in protecting your account as you are because they want you to use them as your primary email address. Yahoo even has its very own site for you to look up that includes information about spam. To get this information see <http://www.yahoo.com/spam>

Most of the free email service providers have similar filters as MSN. They let you control the accepted content, which is exactly what I would advise you to have. They let you decide which mail to let through. MSN Hotmail is currently allowing you to combine the filtering system with a mail washer in their free version. This is how they plan to help you protect yourself from viruses and such; which is great for a free service.

## **Disposable Email Addresses**

Disposable email addresses are a great way to deal with spam. It basically works like this; it is an email address that is generally deletes itself when it finds that it attracts too much spam. It's a low cost way to not have to deal with it at all. The

### The SPAM Files

email deals with it for you. I've enclosed a list of free versions of disposable emails.

- Sneak Email - <http://www.sneakemail.com>
- The Spam Motel - <http://www.spammotel.com>
- Morgle - <http://www.fileheaven.com/morgle-email-link-address-service/download/12689.htm>
- Mailmoat - <http://www.mailmoat.com>



**Where Successful Marketers Meet**

**OnlineMarketersForum.com**

The [Online Marketers Forum](#) is fairly brand new. We already have quite a few active members. Come by and introduce yourself. We are always looking for new members to join us!

**There is NO cost to become a member, so what are you waiting for?**

## **Don't Let Your Password Be Naked! Clothe It With Encryption!**

Encrypting your email passwords is a really good way to protect your inbox from spammer Gangs. Spammer gangs are basically just a group of worldwide spammers that get together online to get into your inbox. However, that is not all they do.

Some spammers make it a point to break into your email and deliver worms, viruses, and Trojans into your inbox. They are cleverly disguised; usually as virus alerts. These types of spammers use hacking to get into your password. Believe it or not, spammers can access your inner email by using your profile and homepage information to access a password.

The best way for you to protect yourself is to use encrypted passwords because they are more complicated to figure out. They are a combination of letters and numbers in your password. For example; if you wanted your password to be sonny, you might want to type s56on976ny instead. It is a little bit annoying to try and remember these types of passwords, but believe me, they are harder to track.

The same rule applies if you want to use all numbers. It is best to add a few letters in it to make it harder for the spammers to decipher. Singular passwords are much easier for a hacker or spammer to dig into and decipher.

## **Pass the Beggars By Online**

You have to admire the spammers interest in pulling at the heart strings in order to get your attention. These are the emails that come from strangers that are from some foreign country who are just looking for “donations” from kind people so that they can finish college or get an operation they desperately need.

These emails are always extremely polite and come from seemingly educated individuals who just need help to make their dreams come true. People must be falling for it since they are still coming out in full force.

You must beware of these pleas for help because they are generally just SPAM scams. Think about it, how desperate can these people be for money if they can afford to mass email complete strangers? I doubt any person who is that poor but can afford a computer and the Internet. Do you ever notice that none of these people even give you a viable home address?

Anyway, this is just a sample of a spam scam, there will be more on this in the next section.

**You're Going TO Get SPAMMED!!!**



## The SPAM Files

As the section above mentioned briefly, there are plenty of spam scams going on out there. These are spam emails that come to you and request money or donations to various charities and such.

These types of spam are illegal. Real charities only use their client contact lists when asking for donations. Spammers will do anything in their power to get you to part with your money. Some of them even offer viable products or services; the catch is that the links to these products or services are rarely usable. Here is a list of some of the spam scams that will ask you for money.

### **Asking for Charitable Donations**

Some even have viable sounding names like the American Heart's Association. (There is no such company) They are relying on the fact that you have heard of the American Heart Association and they have simply pluralized it. It is a really good cover because they know that everyone has heard of the American Heart Association and just changing it a bit causes no real difference to the sound of it, so you are more likely to give up your money.

You really have to watch out for slight name changes like these because these are the scams that are harder to catch. Of course there is one way to know if your email donation request is real. **REAL CHARITIES DON'T SEND MASS EMAILS!**

Don't get me wrong legitimate charities do advertise on the Internet, but they do it on their website alone and generally offer their charity number and a phone number that you can call as well. Be careful on receiving these. If you know that you are a bleeding heart, just don't open them.

Sometimes spammers will get your attention by making the email look like it has been forwarded to you. This is silly really, but it often works because the recipient believes that the email is from a friend or family member. Don't be fooled by the forwarded email. Not all of them are from your friends.

### **Making Money Scams**

Spammers also have a nice running scam that promises you the chance to make some money. These can offer you things like legitimate sounding jobs, and

products. Some of them even have the nerve to ask you in the email itself for your credit card numbers etc.

## **Internet Survey Jobs**

These are just telling you that you can make some money by filling out surveys online. Of course they never tell you that you have to pay a certain amount of money in order to get a list of the legitimate companies that will pay you. Before they even give you that amount of information, you are asked to fill out a registration form, and then your emails from these people will never stop.

## **Online Typing Jobs**

This offers you the chance to type files etc. and receive payment per word or page. Some even offer to pay you by the hour. Ask yourself this; how will they know how long you've been online?

## **Get Paid To Surf**

Everyone has heard of the emails that offer you to get paid just to surf the internet. According to them, you can get paid to go to any website that you want. What they don't tell you is that you have to allow your computer to be hacked into first.

## **Payday Cash Advances**

These are extremely annoying because everyone seems to get these spam scams on a daily basis. These offer to let you receive a payday advance through your email. All they ask is that you give them your banking information like your account numbers etc. I can't imagine anybody being stupid enough to give that information, but many still do. These mails tell you that they need this information so that they can send you your money and also get theirs back later. (Let's just see if you have any money once they are finished)

Some of these warnings may sound repetitive to you, but they are mentioned for a reason. Each and every piece of spam that is sent to your inbox is there to entice you into buying something, or tricks to hack into you computer. They are worth mentioning more than once. You can never be too careful and the deeper you can imbed these ideas into your head the better.

## SPAM FILES

So there you have it. This was everything that you need to know in order to recognize, and get rid of spam; At least from your own inbox. These methods will help you to keep your inbox safe, but it will not completely rid the world of spam.

Right now, there is no sure fire method of ensuring that you will never have spam in your inbox, but for now, there are some things that you can do. If you follow the advice from this manual, you should have at least 90% of your emails be from people that you actually want to hear from. By reading this manual, you have learned how to show those spammers out there that you are in charge of your emails, not them. Good for you!

The advertisement banner features a yellow background with a black border. At the top, there are several 3D-rendered items: a book titled '35 NEW! NEW! NEW! Resources', a book titled 'TECHNOLOGY', a book titled 'Workbook', and two CD-ROMs. The central logo for 'NitroCovers.com' is prominently displayed in a stylized, blue and yellow font, with the tagline 'Give more power to e-Sellers!' underneath it. Below the banner, a white box with a black border contains the following text:

How would you like to have **INCREDIBLE** looking graphics for your site that will make your product or service sell **300% BETTER**? Now you can and you wont have to pay ridiculous prices like the "big boys" are charging! Come by [NitroCovers.com](http://NitroCovers.com) today and see how we can help you **skyrocket your sales** with INCREDIBLE real looking 3D graphics!

With this manual you have successfully learned how to:

## The SPAM Files

- Identify spam when it is put into your inbox.
- Identify the different methods that are used to get through your filters.
- Prevent spam from reaching your inbox
- Recognize the various spam scams out there
- Prevent the acceptance of viruses, worms, and Trojans, into your inbox
- To avoid accidentally sending spam to your friends and family
- How to use password encryption

**Need More Info?**

## The SPAM Files

Below you will find some excellent links and resources to find out all of the information about spam. There will also be some links for you to learn the current spam laws, and get some of the current filters and downloads that will help you win your war against spam.

<http://www.paulgraham.com/antispam.html>

<http://www.paulgraham.com/stopspam.html>

<http://www.internetnews.com/IAR/article.php/2243641>

<http://www.stopspam.org>

<http://www.scambusters.org/stopspam>

<http://www.spamprimer.com>

<http://www.spamarrest.com>

<http://www.spamlaws.com>

<http://www.yahoo.com/spam>

<http://www.boco.net/spamming.html>

[http://www.viralbuzz.com/stop\\_email\\_spam.html](http://www.viralbuzz.com/stop_email_spam.html)

I hope this ebook has given you a good education on SPAM. It's part of our technological world, so you will need to keep your self updated on the latest SPAM tactics! The only true SPAM protection is your know how. Continue your SPAM education and you'll never become a victim of the chaos that SPAM can cause!

Liz Tomey

[TomeyMarketing.com](http://TomeyMarketing.com)