What Spammers Don't Want You To Know About Permanently Blocking Their Vicious E-mails!

Warning: Spam e-mails are not only annoying and time consuming, but they're also becoming more dangerous to your personal and business privacy, and the security of your computer and network. Millions of computer users are getting infected, spoofed, and tricked by spam e-mails every year, forcing the user to pay hefty fees to clean and restore their PCs back to working order.

There are 3 NEW dangers that all computer users must be aware of:

1. An increase in hijacked and spoofed e-mail addresses. Spammers have discovered new ways to make it appear as though their spam e-mail is coming from YOUR computer. This could result in having your Internet connection terminated or put on hold by your ISP - all without your knowledge. That is why a good spam blocking solution will not only block inbound spam from your inbox, but also unauthorized *outbound* spam from your servers.

2. An increase in virus-carrying spam. Accidentally open a spam e-mail carrying a nasty virus and you can end up with big problems ranging from the slowing of your system to more serious threats such as system crashes, data loss, identity theft, redirecting your web browser to pornography sites, and more.

3. Phishing spam. A phishing e-mail appears to be a legitimate e-mail from a bank, vendor, friend, or other trusted source. The purpose is to trick you into giving confidential information such as bank accounts, social security numbers, passwords, and credit card information. You've probably already received a PayPal or bank spam e-mail that said your account was going to be closed unless you verified your information. It then directs you to a very convincing web site where you input certain information the spammer is trying to glean. In reality, this is a malicious third party that is going to use your information to open credit card accounts, access your account, steal money, and cause you other major identity and financial problems.

So what can we do about this?

First and foremost, it is absolutely critical that you get a quality spam blocking Internet-based solution set-up as a first line of defense. The problem with most spam blocking software is that, by design, you have to allow the e-mail into your network in order for the

software to scan it. By having an Internet-based solution, the e-mail goes to a different server first, is scanned, quarantined if necessary, and then the remaining good messages are delivered to you. This will stop the spam or virus from ever even entering your network. New government regulations haven't done a single thing towards preventing or stopping spammers so the responsibility lies on your shoulders.

Next, you want to make sure you don't throw yourself under the bus by getting on a spammers list in the first place. Once you're on a spammer's list, it's impossible to get off; and changing your e-mail address can be a major inconvenience especially if you rely on it to stay in touch with important business and personal contacts.

To reduce the chances of your e-mail address getting on a spammer's list, here are 5 simple preventative measures you can take that will go a long way in keeping not-so-delicious spam out of your in-box.

1. Use a disposable e-mail address.

If you buy products online or occasionally subscribe to web sites that interest you, chances are you're going to get spammed.

To avoid your main e-mail address from ending up on their broadcast list, set up a free Internet e-mail address with Hotmail or Gmail and use it when buying or opting in to online newsletters. You can also use a throwaway e-mail address when making purchases or subscribing to newsletters (see #4 below).

2. Pay attention to check boxes that automatically opt you in.

Whenever you subscribe to a web site or make a purchase online, be very watchful of small, pre-checked boxes that say, "Yes! I want to receive offers from third party companies."

If you do not un-check the box to opt-out, your e-mail address can (and will) be sold to every online advertiser. To avoid this from happening, simply take a closer look at every online form you fill out.

3. Don't post your main e-mail address on your web site, web forums, or newsgroups.

Spammers have special programs that can glean e-mail addresses from web sites without your permission. If you are posting to a web forum or newsgroup, use your disposable e-mail address instead of your main e-mail address.

If you want to post an e-mail address on your home page, use "info@" and have all replies forwarded to a folder in your in-box that won't interfere with your main address.

4. Create throwaway e-mail accounts.

If you own a web domain, all mail going to an address at your domain is probably set up to come directly to you by default. For example, an e-mail addressed to anything@yourdomain.com will be delivered to your in-box.

This is a great way to fight spam without missing out on important e-mails you want to get. The next time you sign up for a newsletter, use the title of the web site in your e-mail address. For example, if the web site is titled "www.greatwidgets.com," enter "greatwidgets@yourdomain.com" as your e-mail address. If you get spammed, look at what address the spam was sent to.

If greatwidgets@yourdomain.com shows up as the original recipient, you know the source since that e-mail address was unique to that web site. Now you can easily stop the spam by making any e-mail sent to that address bounce back to the sender.

5. Don't open, reply to, or try to opt-out of obvious spam e-mails.

Opening, replying to, or even clicking a bogus opt-out link in an obvious spam e-mail signals that your e-mail address is active, and more spam will follow.

The only time it is safe to click on the opt-out link or reply to the e-mail is when the message was sent from a company you know or do business with (for example, a company that you purchase from or a newsletter you subscribed to).

How to Permanently Stop Spam from Taking over your Inbox

As we said earlier, spam has become more than an aggravation; it now poses a serious threat to your computer and your personal security. While the above tips will help some, the only way to permanently stop spam is to have an industrial strength spam filter set-up for you.

But Beware!

Not all spam blockers are created equal, and some can end up blocking important e-mails you want to receive and be a pain in the neck to manage. At a minimum, your spam filtering solution should:

1. **Stop bogus e-mails and viruses from ever entering your network.** If your company's e-mail is hosted locally on your server (such as with Microsoft Exchange), all e-mail whether spam or not, is sent directly to your network. The job of your server (and Microsoft Exchange) is to receive all those messages and send them to the appropriate employee's computer. By design, a spam blocking software allows messages into your server, THEN scans them to see if they are spam or have potentially dangerous viruses. If any of those messages do have viruses, this scanning comes too late; the virus is already in your server. By using an Internet-based spam solution instead, your server is completely protected from ever receiving these harmful e-mails.

2. **Automatically block e-mails coming from invalid e-mail addresses to your domain**. Almost 90% of spam is sent to invalid e-mail addresses at a domain. What is an invalid e-mail? Any e-mail address that is not set up or assigned to a user. For example, you may have 3 e-mail accounts in your organization; one for mary@, one for john@, and one for yourname@. A spammer will often send spam to "info@" or "admin@" your domain knowing that it will get through.

3. **Allow user control**. Make sure your spam blocking solution allows each user to configure their own rules of what should be blocked and what should pass through; after all, one man's trash is another man's treasure! Some spam filters only allow for a "one-size-fits-all" approach and require that an administrator set the rules for a particular inbox. This can be frustrating and time consuming.

4. **Reduce the time you spend on sorting through e-mail.** To be effective, a good spam blocker has to be easy to understand so you can train it and customize it. Find a solution that can send you just one e-mail daily showing statistics of how many messages were blocked and a list of messages you may want to have delivered. This will allow you to easily and quickly deliver messages that may have inadvertently gotten blocked and give you a chance to stop messages that you now annoyingly get over and over again.

5. **Save your e-mails if your server or Internet connection ever goes down.** Though many businesses are not aware of this, if your Internet connection or server goes down and your e-mail is set up on your server, no e-mail messages can be retrieved from your company. This means that any e-mails sent to you during the downtime have no where to go and so are bounced back or simply lost into space, causing serious loss of new business or communications with customers. Your spam solution should offer a spooling service that holds on to e-mails for you until your server or Internet connection is back up and running.