

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

*A report on actions you can take to stop spam BEFORE it enters your network
Author: Darryl McAllister, Managing Director, NetCare HelpDesk*



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

Besides the constant barrage of annoying and inappropriate spam that we all know about, there are 3 major dangers that all businesses 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 good spam blocking software will not only block inbound spam from your inbox, but also unauthorized *outbound* spam from your servers.

2. **An increase in virus-carrying spam**

Spammers have recently begun attaching PDFs to their spam emails, and it's the latest technique being used by spammers in their bid to defeat anti-spam software. This technique works by embedding images within a PDF file attachment and not the body of the email.

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, passwords, and credit card information. You've probably already received a 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 you do about this?

First and foremost, it's absolutely critical that you get a quality spam blocking solution installed as a first line of defense. 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 almost 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 4 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 Yahoo and use it when buying or opting in to online newsletters.

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. And if you want to allow prospects to contact you via your website, get your web designer to create a form that sends an email behind the scenes to your e-mail address.

4. 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).

NETCARE

HELP DESK

How To Permanently Stop Spam From Taking Over Your Inbox

As I said earlier, spam has become more than an aggravation - it now poses a serious threat to your computer network and maybe even the financial security of your business. While the above tips will help, the only way to permanently stop spam is to install an industrial strength spam filter.

Historically, we have provided a number of different solutions to our clients to help them control spam, including software from Microsoft, Symantec, Trend and MailEssentials. Whilst these have done a good job in the past, we note that:

1. they are all getting harder and harder to maintain;
2. each of these programs are adding to the load on the server and are thus degrading overall server performance;
3. more often these days, updating anti-spam software means restarting the server, causing down-time and raising the risk of introducing a problem following a restart;
4. they all place suspected spam in one mailbox for all to say, potentially creating a data security threat for false-positive spam; and
5. newer solutions are now available that stop spam **before** it even gets into the network and onto the server and PCs.

You need Untangle Spam Blocker

Our Untangle Spam Blocker service is the best solution we've found for controlling spam. We install a gateway computer on the perimeter of your network – between your modem/router and your computers – and then we load Untangle Spam Blocker software on that.

Our monthly fee for Untangle Spam Blocker is \$88 (including GST), regardless of the number of users or computers you have in your network, and our fixed-price set up fee is \$352 (including GST). This includes the software and a fully maintained “Untangle black box gateway server”.

We've been using Untangle Spam Blocker ourselves since December 2008, and we love it. And the icing on the cake is that because you're running it all on a gateway server, you're also lessening the risk of your main server running slow, freezing up or crashing completely.

And, if over time you really find it's no good, or we're no good, or for ANY other reason, then simply let us know and we'll cancel the service prior to the next billing with no questions asked.

If you need a cost-effective solution to control spam on your network, then NetCare Untangle is **your** silver bullet.

