

Home Computer **HELP!**

Serving the greater North Hills communities of Pittsburgh
(412) 480-9969 *We make Housecalls!*



Spam and Ham: Taking Back Your Inbox

In computer jargon, “junk” email is called “Spam”, but I’m sure you knew that already. Did you know, however, that the converse (“good” email) is called “Ham?”



OR



Monty Python™ references aside, spam has become a tenacious scourge, overwhelming the volume of legitimate email traffic on the Internet.

Current estimates say that as much as 70% of the approximately 31 billion (!) emails sent every day are spam. This is a staggering increase over the early-2002 statistic of 25%.

So...how do you stop the spam? Sadly, you can't. If you have an email address, you **will** receive spam. Period. You can't open your inbox without getting several unbidden offers to buy potions promising to increase the size of various body parts, cheap designer watch knock-offs, cheap pharmaceuticals or some other such tripe.

Spam exists because it works. Using automated programs, you can send millions of messages per day – and it only takes a few sales to pay for the effort. Real data on re-

sponse rates are hard to come by, but surveys have shown that a surprising 28% of people have responded to a spam email. Even more surprising, 8% of people surveyed have admitted to making a purchase.

The recent high-profile arrest of a spam “kingpin” proves that there are millions to be made in email marketing.

Ok, so what do we do now? The best fix is to drive the spammers out of business by NOT BUYING ANYTHING FROM THEM. As soon as they stop making money, they will move on to something else.

(Continued on page 4)

3-Pronged Defense Against Computer Problems

- Keep your Anti-Virus Software Up-to-Date
- Scan Weekly for Spy-ware
- Use a Firewall

Internet Explorer Keyboard Shortcuts

- **Ctrl-N** Opens a second window without changing the current window. Let's you have two web sites open side-by-side
- **Ctrl-F** Search for a word or phrase on the current web page
- **Ctrl-W** Close the current window
- **Ctrl-F5** Forces a complete reload of the current page

Inside this issue:

Cleanup Tips..... 2

Toss Your Cookies..... 2

Ad-Aware Personal SE Released

If you've talked to us about spyware, you know we recommend both Ad-Aware™ and Spybot Search & Destroy™. When used together, these two programs provide a very strong defense. Best of all, both programs come in “home” versions that are free for personal use (we love free!).

Lavasoft (www.lavasoftusa.com) recently released a new version, Ad-Aware Personal SE. If you are still using Version 6, you should upgrade as soon as you can.

Remember that just like viruses, there are new spyware threats every single day. To

(Continued on page 2)



If you're in the market for a new computer and are tired of the gray boxes that all look the same, call us to design and build a custom computer just for you. Makes a great one-of-a-kind gift for the holidays! How about:

- A completely silent (no fans) computer no bigger than a dictionary
- A stylish brushed aluminum computer about the size of a toaster

Got something special in mind? Give us a call, we can make it happen!

Cleanup Tips

In all versions since Windows 95, Microsoft has included a handy tool called "Disk Cleanup" that helps you get rid of the many and varied temporary files that accumulate over time. To access this tool, open **My Computer**, then right-click on the hard-drive you want to clean. On the menu that drops down, choose **Properties**. On the **General** tab, click on the **Disk Cleanup** button.

You'll get a summary of the various categories of temporary files that were identified. Click in the checkbox next to each category you want to delete, then click on the "OK" button to proceed. We don't recommend

you choose the "compress old files" unless you are extremely low on disk space. Compressed files do save space, but they also slow down your computer when you need to access them since they must first be decompressed before they can be used.

The cleanup utility can also be accessed by clicking on the **Start** button, then choosing **Programs**, then choosing **Accessories**, then choosing **System Tools**, then finally choosing **Disk Cleanup**.



Toss Your Cookies

I'm sure you've heard about Internet "cookies" and how bad they are for you. Let's take a look at what they are, where they came from, and how you can deal with them intelligently.

Cookies are very small, text-based files that allow you to personalize web sites you visit, and store that personalization for future visits. Customizable sites like *My Yahoo* allow you to see, for example, the weather fore-

cast for your town every time you visit the Yahoo site. You might also choose to see most recent closing value of IBM stock, or headlines from your hometown newspaper in Chicago. When you choose to set up these options, they are stored on your computer in a cookie file, and when you load the site in the future, this file is sent to the Yahoo web server automatically so the page can be personalized.

(Continued on page 3)

"The original idea was a good one... Let people have some control over their Internet surfing experience. How did this concept go bad?"



Ad-Aware Personal SE Released

(Continued from page 1)
maintain your defense, you need to use the most current program, and be sure to update your "signature file" at least weekly.

The current release of Spybot Search & Destroy is version 1.3. You can check both the software version and the date of your signature file by choosing "About" from the "Help" menu. If you don't have the latest version, click on the big "Update" button on the main

screen (make sure you have your Internet connection active before you proceed.)

If you're on the Internet often, you should run complete scans with both programs weekly for the best protection.





Toss Your Cookies

(Continued from page 2)

The original *idea* was a good one. Let people have some control over their Internet surfing experience. So...how did this concept go bad?

As you might guess, it took advertising companies (and other more nefarious folks) about 3 seconds to realize this was a great mechanism to find out more about YOU, the target consumer, and track your movements across the Web.

Let's use a fictitious advertising company, Ads-o-plenty, to provide an illustrative example. Ads-o-plenty buys advertising space on popular web sites, like *Yahoo*, or *MSNBC*, or *CNN*, or *Weather.com*. They then sell this ad space to their customers, who might include an investment brokerage house, and a outdoor clothing manufacturer, for example.

Here's how it works. Every time you visit a site where Ads-o-plenty has purchased space, a cookie is stored on your machine that contains any customizations you might have defined, saved log-in information like your name, address, or even a password.

Ok, now for the fun part. As you continue surfing, let's say you go to another site where Ads-o-plenty has purchased space. This site can read the Ads-o-plenty cookie that you have from the first site, and use the combined information to build a profile about you.

"The ad company knows you live in Minnesota in January, so you might be in the market for a warm new coat!"

Let's say you live in Minnesota, and choose to have your weather forecast displayed on Yahoo. If you later visit a site where Ads-o-plenty has sold some of its space to the outdoor clothing manufacturer, and it happens to be January, you might see a pop-up ad for a sale on arctic parkas. That's because Ads-o-plenty **knows** you live in Minnesota in January, so you might need a warm new coat!

Your high-school buddy, on the other hand, lives in New York, and has personalized Yahoo to display the current value of IBM stock. When he visits the very same site you did, he might get a pop-up ad for the investment brokerage. That's because Ads-o-plenty **knows** (or at least suspects) that he owns some IBM stock!

Cookies can be useful (to the advertising companies, not to you!) even if you don't make customizations to web sites. The mere fact that you've **visited** *www.ford.com*, for example, means you might be in the market for a new car.

You can imagine that the profiles made possible by collecting cookies from many sites you visit over a long period of time can be very accurate.

If all of this makes you a little queasy, you're not alone. Queasiness aside though, having a lot of cookies (which can number in the *thousands* very easily) means your computer works more slowly because it has to keep track of them, and web sites load more slowly because it takes longer to sift through 20,000 cookies to find and assemble the 57 Ads-o-plenty cookies.

What can you do about it? Well, to cleanup, you can delete all of your computer's stored cookies. If you are using Microsoft's Internet Explorer (like most folks), Click on the **Tools** menu, then choose **Internet Options** from the list. Right in the middle of the dialog box that pops up is a big, fat button labeled **Delete Cookies**. Remember, though that this will delete every one, including those you might want to keep. The next time you go to Yahoo's site, you won't see your hometown forecast.

A better approach (but much more time consuming) is to click on the **Settings** button, then on the **View Files** button on the dialog box that pops up. This will let you see a list of the cookies stored on your machine. You can click on the column headings to sort the list, and you can highlight and delete any or all entries. If you've never done this before, though, there are probably too many to make this practical. It's easier to delete them all and start over.

Once your machine is free of cookies, you can change your settings to control how and when cookies are stored. Some sites "require" (yeah, right!) you to accept cookies in order to view them, so blocking all cookies will likely mean you won't be able to view some sites.

In Microsoft Internet Explorer, click on the **Tools** menu, then choose **Internet Properties**, and then click on the **Privacy** tab. Here you can deny all cookies, make the software ask you if it's ok to write a cookie to your machine, or choose to accept or deny cookies depending on which web site you are viewing at the time (for example, allow cookies for *www.bigbank.com*, but deny cookies for *Yahoo.com*)

You can also use software packages designed specifically to control cookies (check out "Cookie Crusher" for the PC or "Cookie Monster" for the Macintosh—gotta love those names).

Now you know HOW they work, so you can choose how best to deal with this problem based on your own surfing habits. Good Luck!





Home Computer **HELP!**

130 Pine Road
Pittsburgh, PA 15237

Phone: 412.480.9969

Email: help@home-computerhelp.com

We provide affordable, in-home computer service to customers in the greater North Hills region of Pittsburgh. Evening & Weekends, whenever it fits into YOUR schedule.

Call us for an appointment!

**Repairs, Troubleshooting, Upgrades, Training,
Custom-Built Computers**

WE'RE ON THE WEB!

WWW.HOME-COMPUTERHELP.COM

Spam and Ham: Taking Back Your Inbox

(Continued from page 1)

Legislation is another possible answer. The infamous "CAN-SPAM" law is now on the books. Unfortunately, the impact of this legislation is difficult to gauge. Some argue that the law has actually legitimized spammers by setting out the rules they must play by to be "legal."

Good Practices:

- Don't reply to a spam email. Ever.
- Don't click on the "unsubscribe" links often contained in spam messages. They only serve to identify you as a live, working email address. You'll get more spam by attempting to unsubscribe, not less.
- Don't use a "preview pane" in your email software that lets you see the body of the message without opening it. Just displaying a message is enough to let the spammer know you have a working email address. Set your email to show **ONLY** the subject lines of messages, and delete the spam without opening it.

- For goodness sake, don't BUY anything advertised in a spam email. Never. Ever. Not even just one time.

Software Help

If you use Outlook or Outlook Express, there is free software called "SpamFighter" that works pretty well (www.spamfighter.com). The "Pro" version with a few additional niceties costs \$29.95.

If you use Eudora, you should upgrade to version 6.2, which includes spam-filtering built into the software.

If you use some other software for your email, do a Google search for "Your Software Name" + "Spam Filter".

If you use a web-based email like Hotmail or Yahoo, your only option is to rely on the filters already in use by the vendor.

