

SPAM - NO LONGER JUST FOOD

Remember when email was a neat way to stay in contact with friends and family. It was easy, quick, reliable, and Free. Then the marketing guys got involved and it's no longer free. Now we have to put up with a lot of junk email that we don't want and can't seem to get rid of. Where did it come from? Read on, because in many cases we asked for it. (Note - this newsletter is exceptionally long. You may want to print it for current and future reference.)

In the information age, nothing is free, even though everyone will tell you different. Every credit card, debit card, consumer card, convenience card, etc. creates a list of possible access paths to you. When you request these cards you tell them your name, address, phone number, email address, and lots of other information. These companies that are supposed to be helping you, then sell this information to other companies so you can be targeted in some invasive marketing campaign. Have no cards, you might still be on a list. That's where Spyware comes in.

In this issue we will try to help you guard your system against these invasions and tell you how to avoid them in the future. Some of the things you will read we know you're not going to agree with, but they are still true and will help to keep you safe. We will reinforce the removal of Spyware/Adware, talk about viruses, and review products that will help curb your level of SPAM. Let's go...

I know for a fact that large companies sell the information they collect about you, because I have a convenience card with a major grocery chain and my name is registered incorrectly. Every few months we get a bunch of calls from telemarketers asking for that fictitious person. To date I have not been able to get this company to stop selling my name, or get them to take me off their list. Even if I cancel the convenience card, I will remain on the list, seemingly forever. But, the easiest way to stay off of these lists, is never fill out information about yourself to get a card seemingly for free. Nothing is free!

I know that life is supposedly easier with these convenience cards, and they are not going away, so let's find a way to deal with the intrusions. You have anti virus software to keep your system safe from viruses, but what can you do about invasive non virus junk. Read on...

SURF'S UP

One level of invasion that plagues everyone using Windows NT, 2000, and/or XP is those really annoying little grey popups that offer you goods and services you don't need or want. The best one is the company that wants you to buy software to stop the popups for \$ 19.95 when you can stop them yourself for free. Here is the site with the [Instructions](#).

One site you want to add to your favorites is [Spyware Checker](#). This site has a window to enter the name of the program you are going to add to see if it contains spyware. I tested KaZaA since everyone knows it does and this site reports Cydoor and ebhancer get installed whether you say yes or not. BearShare, another popular peer to peer sharing package has SaveNow embedded in it.

There are many applications available to get rid of Spyware/Adware, but the most popular and the best free one comes from [Lavasoft](#). Of course, only the basic version is free, but visit the site to see all other options available.

Another product to check your system and remove Spybots or Adbots is [Search and Destroy](#). I just downloaded this one and tried it out. Running a laptop with a P4 1.8 GHz I thought would be fast and since it isn't I wanted to know why. S&D found a ton of entries in my Registry and system relating to scavengers looking at my stuff and sending info away from my computer without my knowledge. They also say that BulletProof Software's Syware/Adware remover uses a stolen database (theirs) and therefore I don't think I will use it anymore. S&D Rulez! (at least for now)

Let's turn our attention to email. There are [Spam Blockers](#) available, some for free, and if clicked on the last link you would have found yourself at the [Spam Blockers](#) web site. According to their site "Spam-Blockers.com features the latest and most powerful internet email spam prevention and spam blockers software at affordable prices to help you fight back & stop spam! Spam-Blockers.com is also working on compiling an extensive list of free anti-spam resources."

A search of PC World led me to this site on [Spam Blocking Software](#) that is available, some shareware, trialware, and best of all Free. McAfee even has a product called SpamKiller, but I might just try the free stuff first. Generally when a huge company gets involved their product install a whole lot more that they think you need, when all you really wanted to do was cure the initial problem.

The site [refdesk.com](#) list a lot of software for blocking pop ups, spam, etc. and may be worth a look.

One good way to ensure that you know where you email address is, is never give it out indiscriminently. But I bet almost everyone does. Before you say Not Me! think about the forwarding of emails. I must receive 12 to 24 emails a day of pictures, jokes, jpeg's, notes, etc. that other's find amusing, colourful, entertaining, or whatever. Some pertain to friendship, some luck, others are just funny or interesting but they all share the same instruction. Pass this note on to X number of people in your address list or something bad will happen, or some other such nonsense. This type of note serves two purposes: (1) Clogs up the Internet and slows down servers all over the world trying to keep up with this junk. (2) Releases your email address and a long list of other email addresses to a lot of people you don't know and have never heard of.

HOW? Quite simple. When you forward a received email it logs the list of previous recipients in the body of that forwarded email. Look at some of the one's you have received and forwarded. You have to go through one or two pages of addresses to get to the reason it was sent in the first place. All of these email addresses are now FREE and eventually will get added to mailing lists somewhere. But there is a way to continue forwarding email and clogging up the Internet while staying anonymous. It is the Blind Carbon Copy, or bcc. This option doesn't normally appear on you New Email page, but if you click the To: button in Outlook (Express) to get your address book you will see it there. Select as many names as you want and put them all into bcc. Everyone still gets the email you forwarded, but the only address they may see is their own and yours. Also, when you forward, remember to DELETE the email address of where it came from in the body of the note before you send it, or it helps to defeat the purpose.

TIPS AND TRICKS - OUTLOOK EXPRESS

Using an external product to check and remove unwanted email is only one option. Another, possibly more preferable option is to use the tools included with Outlook Express - such as Block Sender. This utility remembers a set of rules that you create identifying what mail you want to receive and what mail you don't. First we will identify the parts of an address, and then show you how the different parts work.

Email Addresses

An email address is made up of two parts. All descriptions to the left of the ampersand (@) is known as the username. The next part immediately after the @ sign is the domain, and the two or three character suffix at the very end is known as the type of organization. It is probably much simpler to think of the username as before the @ sign, and the domain as after the @ sign.

Simple Blocking

When you receive an email you didn't ask for, simply highlight the unwanted message, click on

Message in to menu bar at the top of the screen, and select Block Sender. You will be rewarded with a dialogue box that informs you that the offending email address has been added to your block sender list, subsequent messages will be blocked, and do you want to remove all messages from this sender now. If you click Yes, all messages in the current mail list will be checked for a match of this senders address, and when identified they will be removed.

This simple blocking method is great if you don't want a specific email address (username@domain.com) to send you anything more, but today companies are springing up which basically are spam servers. Anyone can have one or more addresses and they all get pumped through one server (@domain.com). It is quite common once your address is known to get mail from user1@domain.com and user2@domain.com and - well, you get the idea. There is a way to block everyone from a particular domain.

Domain Blocking

Once you have identified the domain to block, you can set it up in two ways.

(1) Block the original offending site using the Simple method above. Next select Tools on the menu bar, slide down to Message Rules, and choose Blocked Sender's List. This displays the Blocked Senders List of every address you have ever blocked.

Now, locate the address that contains the domain that you want to block and highlight it. Click on the Modify button to display a dialog box of the actual address and the options for applying the block. Point your mouse cursor on the @ sign and click the left mouse button and hold it down while dragging the cursor over the username. Press the Del (Delete) key to remove the username portion of the email address. All that remains is the domain. Click the OK button and that domain will be forever blocked no matter what user name comes in front of it.

(2) The alternate method is to use the Add button on the Message Rules dialogue box. This will display the same dialogue box as above but with a blank address. In the address box, you would type in the domain name you wish to block, select the blocking types, and press OK.

Removing a Block

Occasionally you may block the wrong address. These addresses can be removed by selecting Message from the menu bar, sliding down to Message Rules, and choosing Blocked Sender's List. Again you will see the list of addresses that have been blocked to date. Scroll through the list until you find the address that shouldn't be on the list. Highlight it and press the Remove button. You will be presented with a dialogue box asking if you are sure you want to remove this address. Click Yes if you are sure and mail from that sender or domain will be received in the future.

After the Fact

Some of you may have known about the Block Sender's list for some time but didn't know you could edit it. If you go into the Edit function now, your list could be quite long. Here is where you would do some housekeeping to exclude domains rather than individual addresses to shorten the list. Follow the instruction in Domain Blocking above to edit this list into a shorter one.

While you are doing this, you will probably receive a message that says Blocked sender "domain.com" already exists. Are you sure you want to replace "domain.com"? Always answer Yes to this question. The domains will always be the same and if you answer No, the second address won't be affected.

Whenever you have your system check for email, all the email that is received will be checked against your new list of addresses for validity. It is safe to assume then that the longer your Blocked Sender's

List and the more mail you are trying to receive, the longer it will take to receive your email.

TIPS AND TRICKS - OUTLOOK

Microsoft Outlook is a considerably more sophisticated product than Outlook Express, and as such you can do the same things, but in a different method and broader scope.

Microsoft Outlook can automatically move email from your Inbox to your Deleted Items folder or to any other folder you specify. Outlook creates a folder called Junk Mail, where you can move junk e-mail and then review it before deleting. Or, you can have junk e-mail delivered to your Inbox, but color coded so you can easily identify it. The list of terms that Outlook uses to filter suspected junk e-mail messages can be found in a file named Filters.txt.

You can also filter messages based on the e-mail addresses of junk and adult content senders, allowing you to move or delete all future messages from a particular sender. You can review the Junk Senders list and add and remove e-mail addresses from it.

Junk and Adult Content Mail

To begin Organizing your email, click on Tools on the menu bar and slide down to and click on Organize. This opens the Ways to Organize Inbox drop down screen showing four options: Using Folders; Using Colours; Using Views; and Junk Mail. Click on Junk Mail to see if it has even been set up. If the command buttons say Turn On, this feature hasn't been set up.

Junk mail and Adult Content mail can either be Moved or Coloured to bring you attention to it. My question is, If you don't want it in your Inbox, why colour it? I have selected "move" Junk messages to the Junk E-Mail folder and turned it on by clicking the Turn On Command button. I have selected "move" Adult Content message to Deleted Items and turned it On as well.

However, this doesn't guarantee that you will never receive unwanted mail again. No one can promise that. You must now use the Add function to build your list. When you get an unsolicited message (spam) that you don't want to receive again, highlight the email notifier and click Actions on the menu bar. Slide down to Junk Email and choose the preferred option: Add to Junk Senders List, or Add to Adult Content Senders List. You will be presented with a dialogue box identifying your request has been completed. You can silence this dialogue box by putting a check mark in the square to not show it again.

Editing Addresses

When you want to add new rules to move your email to different folders, or to make changes to your Junk and Adult Content Senders, you need to access the Rules Wizard. On the Tools menu select Rules Wizard to open this option.

Here you will see a list of Rules that have been created, and the folders on which each rule is applied to. When you select the Junk Email Rule the rule description displayed at the bottom of the dialogue box should be "Apply this message after the message arrives, suspected to be junk email or from [Junk Senders](#) move it to the [Junk E-Mail](#) folder. When you click on the Junk Senders link you will open a dialogue box allowing the editing of the email addresses therein.

If you have addresses or domains you want to add, click the Add button. If there is an entry you want to modify, highlight the address and click the Edit button. If you want to remove an entry, highlight it and click the Delete button. One word of caution: There are no prompts here asking if you are sure. Once you click OK or Delete it is done.

Adult Content email works exactly the same as Junk email.

Other Organizational Tips

Microsoft Outlook also allows for organization of email by Folders. Instead of having just one folder, you can create as many folders as you want. Then you create rules for incoming messages to be moved to these different folders. I personally have different folders for my technicals, vendors, TekJournal, and everything just drops into the Inbox.

To create a Folder rule, highlight the email you want moved, open the Organize option, and use the option to create a rule to move new messages... You will have the option of from or sent to, where from is the email address of the sender and sent to is the email address of the receiver. The receiver is a good way to sort email since Outlook will handle lots of different email addresses. Outlook Express wants you to create identities for multiple addresses.

The create rule fills in most of the information for you, you just have to select the folder where it will go. The folder list is a pull down option list with the last choice being Other Folders where you can choose from all your folders, or create a new one. Once you click the Create button that rule is created and all mail matching that criteria will now be diverted from the Inbox to a new location.

You can also use colours in much the same way you use Folders. All your mail stays in the Inbox, unless you have set up additional movement rules, but you can assign colours for different messages and for different email addresses. I don't use this option, preferring the Folder method more.

VIRUS UPDATES

June 4 - The W32.Bugbear.B@mm worm is upgraded to a Class 4 threat. The W32.Bugbear.B@mm worm is a variant of W32.Bugbear@mm. It is defined as a mass-mailing worm that also spreads through network shares. It is polymorphic and also infects a select list of executable files. It is very serious in that it possesses keystroke-logging and Backdoor capabilities and will attempt to terminate the processes of various antivirus and firewall programs. The worm uses the Incorrect MIME Header Can Cause IE to Execute E-mail Attachment vulnerability to cause unpatched systems to auto-execute the worm when reading or previewing an infected message. Because the worm does not properly handle the network resource types, it may flood shared printer resources, which causes them to print garbage or disrupt their normal functionality.

VBS.ExitWin was discovered on June 5 and is a threat Class 1. It is written in Microsoft Visual Basic. When it is run, the script asks a series of questions in Malay. If you enter the "wrong" answer, the script closes Windows.

W32.HLLW.Nool@m, also discovered on June 5, is a worm that attempts to spread itself through email. The worm replies to the first email it finds in Microsoft Outlook. The email will have a variable subject and attachment name. The attachment will have a double extension, the last of which will be either .com, .exe, .pif, or .scr. This worm also contains a Backdoor capability and it attempts to connect to a specified IRC channel on port 6667.

June 5th was popular with viruses as **PWSteal.ABCHlp** was also discovered. It is a password-stealing, Backdoor Trojan Horse. The program attempts to send password information from a compromised computer to an address in China. By default it makes use of ports 1025 and 1027.

Viruses are potentially harmful to all systems and should not be treated lightly. Connections to the Internet that have the capability of 24/7 (cable, DSL, etc.) should be protected by a hardware firewall. All systems should be protected by a qualified anti virus software product. We recommend Norton.

There are “free” products available but you get what you pay for.