

Junk eMail

In the world of "spam" (un-requested eMail) there is no sure-fire method of stopping all unwanted eMail. However, there are a few things you can do to slow it down a bit...

Don't Open It

When looking at the list of eMail, notice the "Subject" and who it's from. Sometimes you may not know it's junk mail from one or the other but putting them together with a sprinkle of detective-style thinking may help determine if a piece of eMail is worth reading or should be deleted. Here are two examples:

eMail Address:.....Subject:
bankmanager@y3itm-46dtx.com.....Re: This month's bank statement
bankmanager@citibank.com.....problem with your check
account.....lkf3khp-xeuk

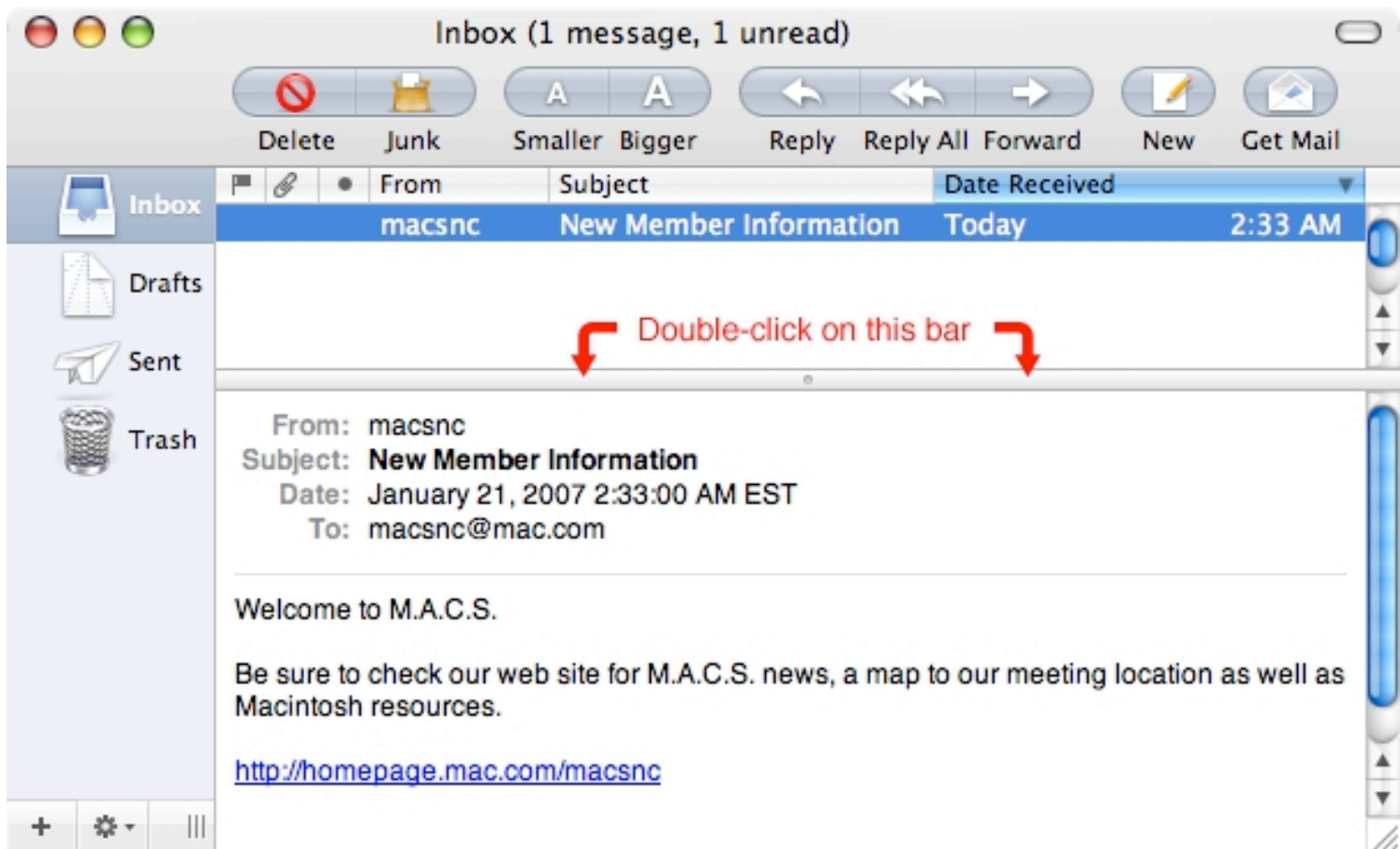
In the first line, although the "bankmanager" part of their address looks good, everything to the right of the @looks suspicious. This is junk mail. Don't open it.

In the second line, the entire eMail address looks legitimate but the Subject line starts us thinking. (Yes, spammers (junk-mail Senders) CAN forge an eMail address to make it look authentic.) First of all, if there was a problem with your account, the bank would most likely phone you or send you a letter in the mail. The words "problem", "need your help", etc. from a suspicious Sender should be avoided and not opened. Just delete it. Also, sometimes a junk-mail message will have a long space after the Subject and then some strange characters to the right. If you don't see them, place the Pointer over the bottom-right corner of your mail window (where you see your current list of eMails) then hold down the mouse button and drag to the right. This will make that window wider enabling you to see if there are any extra characters to the right of any Subject line.

Remember, if you know you have found a piece of junk mail, DO NOT open it. DO NOT reply to it. If there is a horizontal bar separating the message "list" from the message "content", double-click it (see illustration below). This will send it to the bottom of that window. Now, when you click on an entry in the Message List, the eMail won't open (its contents won't be displayed). This is important because sometimes junk eMail can send a note back to the Sender informing them that you opened their message. They will then add you to their "real" eMail list and send you more unwanted eMail. Yes, this can happen simply by you opening a message.

- Regarding the word "real"... Some junk eMail Senders use a computer program which generates eMail addresses. The Sender doesn't know if any of them are real addresses so lots of special messages are sent out to those people. If anyone responds or, if the message has been programmed to "report back", they will know yours is a "real" eMail address.

While the Mail List / Mail Content divider is at the bottom of that window, just click once on any junk eMail then click the "Delete" button. By doing it this way, you won't be opening the message. You'll just be deleting it.



- NOTE: Your eMail window may look different. Each version of Apple's "Mail" program has a slightly varied look. The Mail List / Mail Content divider will work the same as the one above.

- The Mail List / Mail Content divider can be dragged Up or Down but double-clicking it will quickly drop it to the bottom of the window. When it's at the bottom, double-clicking it will instantly move it to its previous location.

Block Spam Yourself

Apple's "Mail" program allows you to set up your own criteria for blocking junk eMail. Pull down the "Mail" menu and select "Preferences". In the dialog box which appears, use the "Junk Mail" and "Rules" buttons (across the top) to configure these settings. Pull down the "Help" menu to learn more about how to do this.

Take Responsibility

Each of us must make sure we do not contribute to junk eMail. How? Two ways come to mind...

Stop Joking

First, I know all of you mean well but PLEASE stop sending your loved ones eMails about your favorite JOKES! We've all received these but believe me, there are probably HUNDREDS of web sites with tons and tons of great jokes. If someone sends them to you, please stop the chain and just delete it.

Yes, I know there's not enough laughter in the world and everyone could use a good smile. That's fine but what you're really trying to do is tell that person "Hey, I was thinking of you today", or "How's the weather where you are?" or "Remember that great time we had...".

eMail doesn't convey those nuances we create with our handwriting when we used to send letters through the Post Office. It doesn't provide the detail, emotion and excitement we deliver when we talk on the telephone. Trying to lighten someone's day by bombarding them with a hundred of the best jokes or one joke every day or so will probably just annoy them.

There's no need to hide behind a list of jokes. Tell them how you really feel. Tell them you care about them. This will mean a lot more to them.

Just BCC

Whenever you send eMail to more than one person, BE SURE to mark EVERYONE as BCC (Blind Carbon Copy). Just about every eMail program, AOL's included, will allow you to send to someone as "TO" or "CC" (Carbon Copy or Courtesy Copy) or "BCC".

When sending a message to ONE person or ONE company you really don't have to do anything. The default for most programs is "TO".

When any of the recipients read your message, they will not be able to see any eMail address which had a "BCC" next to it.

Why is this important? Sometimes one or two people you sent a message to will send their own message to everyone on that list. Even if they don't. Most likely someone on your list will click the "Reply All" button and send a response to EVERYONE! or... They will click "Forward" and send this to someone else. When they do this, guess what?... That next person will see EVERYONE's eMail address which did not have "BCC" next to it. We've all gotten this type of message! Sometimes one group sends to someone who sends to another group, and so forth. At some point, there are SO MANY eMail addresses listed that no one can find the MESSAGE!

Please practice "BCC"!!!

If someone sends me a group mailing without listing me as "BCC", I will politely explain the ramifications to the sender. I will then make a note of "who" sent me this and "when". Then, if they ever send me another without listing me as "BCC", I immediately go to the Preferences section of my Mail program and block all eMail from that person. I'm sorry but junk eMail is difficult enough to deal with without someone unknowingly distributing my address throughout the Internet kingdom.

"Dial-Up" and "High-Speed" Technology

"Dial-Up" is when a computer connects to the Internet or sends & receives eMail using a standard telephone line.

"High-Speed" (sometimes called "broadband") is when a computer accesses the Internet or sends & receives eMail using non-dial-up technology, usually: cable modem, satellite or DSL (digital subscriber line, through the local telephone company).

Dial-up users will experience more and more partial web pages as well as "timed out", "too many requests pending" and "host not responding" messages. You may even click on a link and nothing will happen.

All of this is because more and more of the world is moving to high-speed Internet access.

When anyone clicks on an Internet link, a request is sent to a computer (a server) on the Internet which is supposed to direct you to that web page. Since these servers receive thousands of requests per second, the high-speed requests can explain what they need before a "dial-up" request has gotten the server's attention.

Before long (around 30-seconds), the server sees that it has a partial request (from a "dial-up" computer) but has to throw it out (ignore it) because too much time has passed. Sometimes you'll receive a "proper" message explaining "too many requests pending", etc. Other times nothing will happen.

This is an over-simplified explanation but it's what's happening more and more. I spoke with someone today who had this same issue. He thought there was something wrong with his iMac. He has AOL (America Online) and phoned them to see what could be done to fix it. They told him he needed a new Browser. (He's using the highest version of AOL for his iMac's OS 9.) He also told me he first tried to access a few web pages in the morning but nothing happened (no messages or errors). He then made a few phone calls. A few hours later, he tried those same pages again and they came up just fine.

It's really too bad that more and more people are being forced into spending extra money on high-speed access when all they really want is to send and receive eMail and browse a few web pages.

AOL does offer high-speed access but the last time I checked, it was only for PCs. We were on AOL for 15-years. I even beta tested it when Apple initially started it. At that time it was called "AppleLink Personal Edition". Around April 2003 we switched to BellSouth's DSL service. It's about \$55 a month -- compared to AOL's dial-up service for \$23.90. Before we switched, we researched cable, DSL and satellite technologies and found DSL to be the best for us. However, not every location can use DSL. To find out if your location can subscribe to DSL, go to: <http://www.fastaccess.com>

This page allows you to enter your phone number and within seconds it will tell you if that location can subscribe to DSL.

Virus Protection

Apple has made every effort to protect our beloved Macs from the negative influences in the outside world. They constantly stay on top of this and seem to patch potential "holes" before most people even know they exist.

- Virus: Software which purposely performs malicious tasks inside a computer. (Such as delete files, send junk eMail using your own address book, etc.) There are a few virus "categories", worm, trojan horse, etc., but they all come under this definition.

Viruses are usually employed simply to cause problems and panic and sometimes just to see if such a program can be created -- the "thrill" is in the doing. Others will create viruses simply for the glory. The further a virus travels around the world and the more people make a big deal about it the more excited its creator becomes.

- **Hack:** To break into a computer. To bypass, trick or change software to gain access to a computer and the information it contains. Some hacks are performed "remotely". A program is sent out, randomly or directly, (over the Internet or network) to search for specific flaws or "features" in another program which would allow access. Once this is accomplished, information from the hacked computer is sent to the Hacker -- the person who originated this process. Hacking can also be performed directly... A person, using various hacking or monitoring programs will control this software in real time and instruct it where to look and how to accomplish its tasks.

Hacking is usually performed in order to locate personal or secret information -- credit card numbers, etc. This data will then be sold or used by the Hacker.

NOTE: If your Macintosh accesses the Internet via a high-speed connection, visit the following Symantec page. Scroll to the bottom and click "Check for security risks". Within a few minutes, it will diagnose your Internet configuration and provide a report explaining which areas, if any, are vulnerable to attack.

http://www.symantec.com/nav/nav_mac/index.html

NOTE: Since viruses and hacks can be more easily performed on software which contains security shortcomings (loopholes) and because microsoft products are well known to contain such "features", I STRONGLY recommend NOT using, installing or even keeping ANY microsoft programs on your hard drive!!!

Protecting Ourselves

Although nothing is ever 100% secure 100% of the time, there are ways to lessen our odds of becoming a victim to these tactics:

Virus Protection Software - Installing this type of program in your Macintosh will keep an eye on suspicious activity. A good program will give you the option of automatically checking EVERY file that's opened, downloaded and decompressed.

Of the 3 anti-virus program I am aware of, I would recommend Symantec's "Norton AntiVirus" (Keep in mind I do NOT recommend Symantec's "Norton Disk Doctor" utility!)

Firewall - A Firewall will protect your computer from being hacked. I'm told you get the best Firewall protection simply by using a "router". This is a piece of hardware about the size of a postcard but an inch thick or so.

NOTE: If you're using "dial-up", a standard telephone line, to connect to the Internet, you cannot use a router for this purpose.

If you have high-speed access, your modem may include Firewall protection. If it does, don't buy Firewall software. I'm told this will not give you twice the protection but it will cause problems instead. If you just need Firewall software, activate the Firewall features found in the "System Preferences" section of Mac OS X.