



ADVISE FOR VICTIMS OF SPAM

FREE SPAM FIGHTER TOOL:

http://www.spamfighter.com/Product_Info.asp

If you believe you are a victim of e-mail abuse? This is a step by step procedure on what to do!

Email Spam is **unsolicited commercial email**. Spammers steal mailing lists or acquire addresses from usenet postings or other places on the Internet. This is the most common form of Spam.

Unsolicited commercial e-mail- Any e-mailed document or documents consisting of advertising material. This is what is often referred to as Spam. **Spam** - The electronic equivalent of junk mail.

Harassing e-mail can take a number of forms. Mailbombs are one method. Threatening, abusive, obscene or vulgar messages are other examples. Some Email Spam may classify as abusive or harassing as well. Have you been receiving harassing or threatening e-mail? Please read our section on **Harassing E-mail** to find out what you can do about it.

A **virus** is a program that infects a computer by attaching itself to another program and propagating itself when that program is executed. They can be spread easily through e-mail and wreak havoc on computer systems. If you think you may have been given a virus visit: <http://us.mcafee.com/>.

HARASSING E-MAIL

Harassing e-mail can take a number of forms. Mail bombs are one method. Threatening, abusive, obscene or vulgar messages are other examples. Some Email Spam may classify as abusive or harassing as well.

Mail bomb- massive amounts of email sent to a single system or individual. This is usually done to crash the user's system. Mail bombing is one step beyond flaming and can on many systems result in the cancellation of the bomber's account.

Many harassers (aka: Cyberstalkers) go to great lengths to conceal their identity too. They may use the conventional methods such as sending messages through an unsuspecting third party, or use tools that allow messages to be sent anonymously. There are even web sites that generate abusive, anonymous hate mail. However, it may still be possible to find out the source of the message. Please read **Identifying the sender** below.

Even if you cannot identify the sender you still may be able to put an end to it. Some states are passing laws specifically against email harassment, while other states' existing harassment laws include electronic harassment. For example: In Maryland, cyberstalkers can be fined \$500 or receive up to three years in prison. The Information Technology Association of America lists each state's obscenity, harassment and child pornography laws as they relate to the internet.

Know your rights under the law. If you have been harassed, do not hesitate to call the appropriate authorities. They have ways to find these people! You do not have to remain a victim! Please read how to **Report Abuse** below.



IDENTIFY THE SENDER

Many people inaccurately believe that the sender of the message is the one listed in the "from" line. The problem is that spammers can forge the information in the header. The following is an example of header lines and what to look for in order to accurately determine the origin of the message. In order to view this information you must be able to view the entire header. In **Netscape** select "View>Headers>All". In **Outlook Express** open the message and select "View>All Headers"

Message_Id: Look at the domain name ("userABC@123domain.com"). These should agree in different areas of the header. An exception to that might be if the individual has his own domain name then the Received and ID would show the service provider's domain name while the other areas show the individual's domain name.

The most valuable information you have is in that last "Received:" line. Unless the user can control that domain the domain name and IP address (ex: [200.194.2.160]) should be accurate. That IP address is going to be the source of the message.

REPORT ABUSE

This is the most important step in the process to help put an end to Email Abuse. Contact the service provider directly in hope of getting the offender's service terminated and/or do the following:

To report fraud contact the Federal Trade Commission at: <http://www.ftc.gov/>.

To report the abuse in you particular state contact your Attorney General at: <http://www.findlaw.com/11stategov/indexag.html>.

Keep in mind that we are only here to help and offer information for your use, not to do the work for you. Due to the number of reports we receive daily, it would be impossible for us to handle each individual case. Please consult the following guidelines before reporting abuse instances to ABS Technologies.

1. If you know the ISP of the abuser please do not forward the report to ABS Technologies. You need to contact the ISP directly, as we do not have the authority to do so for you.
2. If you do not know the ISP of the abuser and have not yet viewed all headers and traced the originating IP address, please do not forward the mail to ABS Technologies. We offer complete step by step instructions for tracing the IP address on our site. Please try to follow those first.
3. If you are receiving spam (pornographic or otherwise) from or to an AOL account, for example, please do not send it to ABS Technologies. The problem of spam and AOL accounts is larger than anyone can handle individually. You would benefit more by forwarding all of the spam to AOL themselves and YOUR STATE CONGRESSMAN. It is a huge issue that will only be resolved by government involvement and/or effort on the part of the Internet Service Provider. You, the users have the power to end this problem by speaking out.
4. If a person is harassing you and you feel you are at risk of physical harm, please contact your local police. We cannot help you and will always direct you to the authorities in this instance. Please do not leave yourself at risk, contact the people who can protect you and have the legal means to catch the abuser quickly.