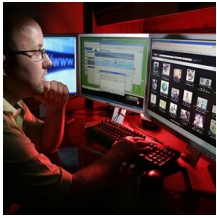


28 July 2008

By: George Craciun, Security News Editor



McAfee advises on how to stay clear of spam  
Michigan Live

## [McAfee Advises on How to Avoid Spam](#)

### *Most spam messages try to get your machine infected*

Nobody wants to login to their email address and find the inbox chucked full with spam messages, especially since said messages are sent out in order to propagate all sorts of malicious software. Most of the times the goal of the spammer is to infect your machine, turn it into a zombie PC in an ever increasing botnet. According to McAfee, company that specializes in risk management and intrusion prevention, there are three things that you must keep in mind in order to stay safe: the most used spam subject lines, the categories they relate to, and a few tips and pointers meant to keep you safe.

**Current Spam Categories** As a rule of thumb, spammers will resort to pretty much any trick they can come up with in order to propagate their malicious intents. According to a study recently updated by the McAfee team, the top three spam categories are products and services (36%), adverts (30%) and stock (11%). Other categories include Russian spam (10%), adult services (7%), and last but not least IT related and financial (both 3%). McAfee also included news and Chinese spam in the list of categories, but they ranked in at 0% (perhaps such categories are not very active in July).

**The Most Common Spam Subject Lines** Generally speaking, spammers will use any high profile event or any piece of news that might be of general interest, such as the [earthquake that devastated China](#) earlier this year, to make up bogus spam messages. Whenever a celebrity makes the headlines, such as [Angelina Jolie](#) after the release of "Wanted", they once again start sending out messages that promise to show her in an unflattering way (most of the times in circumstances that can only be viewed by adult users). Here are some of the most used spam subject lines: "Cheap rolex, omega, cartier...lowest prices; Raw video of Paris; Look attractive with larger jackhammer; Woman loses nose after dog attack; Stay stronger and harder." Pretty much every unsolicited message advertising some adult footage of a well known celebrity is spam.

**Tips and Pointers to Avoid Spam** If you have to make your email address available to the general public, and by that I mean putting it up on the web, make sure to obfuscate it. Instead of John.Smith@mail.com use the obfuscated version John.smith -at- mail -dot- com. An even better idea would be to use graphic image that depicts your email address. Do not use the same email address for work related activities and for personal ones. You should have at least two, separate addresses and use them according to the situation. If you want to contact your friends or coworkers then use one email, if you want to post messages on forums or subscribe to newsletters use the other one. If your Internet service provider offers spam filtering, [McAfee](#) suggests that you enable this option. If any spam messages get through the filter, you should report this to your ISP. Do not provide your email address to any site unless you have read the privacy policy and you agree to it. You must make sure that the web page in question will not sell on your email. When you receive a spam message, do not open it, do not download any attachments it may include, and never answer back. By replying you are only providing the spammer with confirmation that the email is active, that you are using it frequently. If a spam message informs you that you need to update your profile info, or verify your bank account details, that message is definitely a phishing attempt. If you click on the web link included in the message you will be directed to a phishing site where the attacker will try to obtain your security credentials. Your login details are yours to know, and nobody else should get hold of them. Do not give out your username or password to anybody, no matter who requests you to do so. Make sure to update your security software solution on a regular basis.