

By: Fedor Orlov, SEO News Editor

[Spammers Find Way to Beat Filters](#)

The new tactics are rather ingenious

The usual spam message is easy to recognize for those with the minimum level of know-about, and there aren't many Internet users nowadays that lack any interest in the matter. The methods and techniques used by cyber criminals must evolve continuously because the security companies are hot on their tracks in finding and unmasking the dangerous content. Just a couple of days ago, I wrote about the [best Gmail hack found to date](#), that manages to fool captchas and create scores of new legit-like email addresses. McAfee just found out that spammers are going for that exact very legit-like approach by using out-of-office auto-responders to sneak their emails to beat spam filters. The key is to fake the messages to appear as being sent from popular email applications. Only the address is normal, however, and will get the email through. Once the email is opened, it's the same old story over and over again, with lots of advertising and more often than not, adult sites are involved as well. Clicking on them will of course send the user into the arms of desperation, as all hell will break loose with Trojans and spyware."Interestingly, we see spam from a number of accounts being abused in this way. I suspect the spammer has a program that automatically creates accounts and sets the responder text, all with no manual work required. This gives the spammer the capability to have lots of webmail accounts, all used to spam lots of people," McAfee anti-spam engineer Jeremy Gilliat said. The strongpoint of the scheme is exactly the difference between the messages being sent by botnets, opposed to those sent through regular email services. One will probably get caught in the filter while the other might flourish an infestation of the user's computer. Not looking bright.