Spam Procedures & Solutions

There has been an incredible increase in the amount of spam coming to our mail server. We've also gotten feedback from you, our customers, about your frustration with the volume of spam you are receiving. You've also expressed concern that a great deal of spam contains viruses and exploits (i.e., Trojans, worms, backdoors) that could allow unscrupulous people to gain access to your computer. This seemingly unending increase in the volume of spam has begun to adversely affect the mail server's ability to send and deliver your mail effectively and efficiently because much of its resources are being used to process spam.

Based on your requests to "do something" about all of the spam you receive and to help us meet our goal of providing you with exceptional service, we are implementing new measures to combat spam and improve your email services. The explanation below details these new measures.

Our email server runs several email filters which are being deployed as the first line of defense for your email service. These filters are detailed below. You will retain your ability to manage further Spam settings on your own through the Surgemail features already in place.

Blacklists

A Blacklist is a database of known Internet addresses (or IP's) used by persons or companies sending spam. These lists use various methods to identify spammers. For example, one of the lists identifies spam that is sent through sites called "open relays." These sites will accept email from users not on their site for users also not on their site and forward it to them. Open relays are used mainly by spammers to obscure where the mail is originating. Worse, they can deliver a single email to an open relay and address it to hundreds of recipients, thereby causing the open relay to do most of their work. With this blacklist in place, the mail server will reject mail coming from open relays. Such email will be rejected with a message to the sender. If you hear from someone whose email to you has been rejected, please ask them to contact their mail administrator who can go to the site below to find out how to be removed from the list(s):

- sbl-xbl.spamhaus.org - see **http://www.spamhaus.org/**

Attachment Type Blocking

For your safety in using email and to help prevent the spread of viruses and other exploits, we also block the following attachment types: exe, com, scr, vxd, pif, vbe, vbs, vbx, cpl, xl, bat, cmd. These are all known to be used by viruses.

If you need to receive an attachment with a file which uses these blocked extensions, we recommend that you ask the sender to zip the file before sending it. The sender may also change the file extension to zzz which you can then rename upon receipt. If you choose this option, make sure the sender provides you with the correct file extension so you can rename the file properly.

Virus Scanning

We scan all incoming and outgoing email which traverses our mail server for viruses using MPP+Sophos virus scanning engine. For more information on Sophos, visit **http://www.sophos.org/**.

If you have any questions about these new procedures, please email **support@rose.net** or call our Technical Support team at one of the numbers listed below:

- **Cairo:** (229) 377-9515
- **Camilla/Pelham/Baconton:** (229) 336-7857
- **Moultrie:** (229) 891-3264
- **Thomasville:** (229) 227-7086

Thank you for the opportunity to serve you.