

SPAM – A word that used to conjure up fond memories of a particular mystery meat that originated in 1937 has recently become one of the most irritating aspects of our everyday email experience. It has also become one of the most irritating aspects within the small office computer networking firm experience. Why? Because there is no way to 'win' against spammers. It goes like this: if people receive a lot of spam every morning they complain about their email hosting service, but if you put a really stringent spam filter on their email then they complain that their emails are not going through to and being received from customers and vendors, etc. So, the question ends up being: which is more important to you? Knowing all your legitimate communication is working and deleting more junk email in your Inbox or having less to sort through and the possibility that you may not be receiving all your legitimate emails and that the emails you send may not get to their destination either. Oddly enough the answer I most commonly hear is that people want to receive less junk even if some of their mail doesn't go thru or they don't receive some from customers and vendors. This seems amazing to me because the same customer was just fuming because they missed a huge order a month earlier. I try to explain to people it is a lot like your physical mailbox, and I personally would like someone to go thru all the incoming junk mail, sort it out and throw away all those pieces that I don't want to see but that doesn't happen. We are all used to this so why is it so much harder to do it electronically? Let's take a look at the definition of spam today and why it has become such a huge issue.

Wikipedia, the free online encyclopedia, defines **spamming** as the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. Statistics consistently show that at least nine out of ten emails received at any given time are spam and that spam traffic has risen 44% in the first three months of this year. Most of this comes from what is known as 'directory harvest attacks' where harvesting companies take valid domains and generic phone book data to form thousands of possible email addresses for that domain. Add to this is the fact that most addresses people select are usually first initial and last name or first name and last initial. If a potential combination is invalid the email server automatically returns a 'not found' message to the sender, if no 'not found' message is returned the address is tagged as valid and added to the spam database. This is how spam can find its way to a new email address within minutes of it being setup.

According to the Federal Trade Commission: To find out which fields spammers consider most fertile for harvesting, investigators "seeded" 175 different locations on the Internet with 250 new, undercover email addresses. The locations included web pages, newsgroups, chat rooms, message boards, and online directories for web pages, instant message users, domain names, resumes, and dating services. During the six weeks after the postings, the accounts received 3,349 spam emails. The investigators found that:

- - 86 percent of the addresses posted to web pages received spam. It didn't matter where the addresses were posted on the page: if the address had the "@" sign in it, it drew spam.
- - 86 percent of the addresses posted to newsgroups received spam.
- - Chat rooms are virtual magnets for harvesting software. One address posted in a chat room received spam nine minutes after it first was used.

Addresses posted in other areas on the Internet received less spam, the investigators found. Half the addresses posted on free personal web page services received spam, as did 27 percent of addresses posted to message boards and nine percent of addresses listed in email service directories. Addresses posted in instant message service user profiles, "Whois" domain name registries, online resume services, and online dating services did not receive any spam during the six weeks of the investigation. You can also report spam to the FTC by sending it to spam@uce.gov. The FTC uses this information to pursue law enforcement actions against individuals who send deceptive spam.

There are several other websites working to fight spam where you can report it as well: www.spamhaus.org, spam.abuse.net, www.killersites.com to name a few. Also, do not send 'remove me' or opt-out responses to spam messages even when it includes removal instruction unless you are absolutely certain who the sender is i.e. an email list you signed up for previously. This confirms your address validity by giving the spammer a 'confirmed deliverable' and increases the \$\$ value to the spammer as well as the odds it will get sold to additional spam lists. A good rule of thumb is: if you did not opt-in do not opt-out. For additional information regarding spam and ways to fight it please contact Carin Slader at cslader@med-data.com or 864-297-8889.