SPAMFIGHTER SURVIVAL GUIDE

"NO ONE PERSON, COMPANY OR PROGRAM CAN ELIMINATE ALL SPAM ALL THE TIME, UNLESS YOU SMASH A SERVER TO BITS, NEVER TO BE USED AGAIN" - Anonymous

How to Deal With Friendly Fire Effectively

Quite often at the worst possible time, you receive complaints from your end users wondering why or how a certain spam email came through to their inbox. While we have no solution to stop the complaints, we can help you win friends and handle the complaints graciously.

It's important to keep in mind that end users are, for the most part, good, honest people, and in many cases just need a little help and handholding. You know that the typical end user has no clue about the breadth of the problem they are experiencing. For the most part, they are largely concerned only with the basic systems and tools they use on a daily basis to perform their required work tasks. So, always start by ingratiating yourself to them and communicate with an end user delicately, speaking their language slowly, deliberately and respectfully, no matter how funny, outrageous or completely oblivious their comments are. For example:

"Ok, let me understand this - you've received an email that you think is spam or another Internet threat and you don't know how or why you received it. You understand that we have filters and protective measures in place, but don't understand how this one email made it through. No problem, allow me to explain."

To help maintain your composure and keep from rolling your eyes or groaning out loud, keep the following ideas in mind when fielding end-user complaints:

- First and foremost, it is impossible for anyone, anything or any company to eliminate all spam all the time.

- Most end users just browse the Internet and check email (the rest of their job exists in the MS Office world).

- Occasionally, an end user is quite confident he/she knows what they are talking about, but uses IT terms that are not relevant. (Write down these "best misused" terminologies to share with your colleagues or add to your end-user "wall of fame".) Acknowledge that you hear them and that you appreciate them using "tech-talk." Ask them to tell you

MARSHAL™
Secure. Protect. Comply.

again using layman's terms and sparing no details, because you want to ensure that you completely understand their exact problem.

- Invite users to join in the war on spam. Set up an internal inbox and encourage them to forward false positives to notspam@yourcompany. com which is set to autoforward to notspam@marshal.com.

- Resist the temptation to grab the user's PC, run it wildly to the rooftop, and smash it to the ground to cast out evil spam spirits. Your goal should be to educate the end user so that their future IT troubles are succinct and helpful to you in identifying the problem and required solution.

- It is a war not a battle: you're in for the long haul because spam is increasing in complexity and quantity.

- The only perfect solution to spam is to shut down all email and turn off your Internet connection.

War Room Tactics and SpamFighter Simulation Training

Below are common complaints, which you probably receive over and over. With an energetic, relaxing and engaging tone, you can easily dispatch complaints, educate the uninformed, and win the respect you deserve. But, be careful, you might develop a fan club that starts calling and stopping by regularly to chat about their view on security and technology (and in their "speak").

Situation: The VP of the company where you work has just received two emails inviting him to try the new Viagra 4000 Power Pill. Perturbed and irritated by this attack to his email inbox and manhood, he stomps down the hall to your desk and demands an answer to this situation.

Proposed Response: Great question, forward the email to spam@ yourcompany.com (which you secretly auto-forward to spam@marshal.com) so that we can get the offending message to our vendor for analysis. In the meantime, we will send you the latest report showing that for the one spam that made it through, more than 200 others were blocked for you today.

Situation: CFO comes into IT office and asks why he is still getting some spam since the purchase and implementation of the email content security solution.

Proposed Response: I understand the frustration but it is important to understand the situation regarding spam in the world today. Our company alone blocked [insert big number here] spam messages last week and, according to Marshal's team of security experts, Threat Research and Content Engineering (TRACE) , spam is still on the rise. I can assure you that we have implemented all of the recommended policies and are blocking as

M★RSHAL™

Secure. Protect. Comply.

much spam as possible while ensuring none of your important incoming and outgoing emails are delayed or displaced.

Situation: Jane from accounting realizes that she did not receive a legitimate email from a business partner. Understandably upset, she calls the helpdesk (HD). Here is what transpired:

HD: Thanks for calling the Help Desk. How can I help you?

Jane: I just got a call from Bob at Important Business Partner X wondering why I never replied to his email. I never received an email from him. What the heck are you IT people doing to my email?

HD: I see. Did you check the Spam Quarantine Management website to see if it was inadvertently blocked as spam?

Jane: Uh, no! Isn't that your job?

HD: Well, Jane, we respect your integrity, deadlines and the confidential or sensitive data that you must deal with, so, we implemented a website that permits you to easily access, review your blocked email and release legitimate email WITHOUT HAVING TO CALL THE HELPDESK. We thought it could speed things up and save you some time. You like to save time right?

Jane: Well, um, of course…

HD: Of course you do. You can also add email addresses to your personal white list to ensure that emails from Important Business Partners always make it to your inbox. Let me help you release Bob's message and add him to your white list so you don't have this issue again.

[Walks Jane Through]

Jane: Wow that was easy!

HD: Now, is there anything else I can help you with?

Remember: Fighting Spam – It's a War Not a Battle

The nature of the spam beast is to clog email inboxes with as many useless and, increasingly, malicious emails as possible. It can be overwhelmingly frustrating to locate legitimate messages when having to dig through massive amounts of spam. Effectively building a brigade to battle this nonsense, Marshal understands the battle-terrain and guerilla tactics of the enemy and has been fighting this war for more than 10 years. It is a war where we help you consistently win 99.5 % of the time.

M★RSHAL™
Secure. Protect. Comply.

Many end users don't understand the complexity of this fight, so educating them and showing them how successful you are being with MailMarshal will calm them down and let you focus on the 80,000 other items on your plate.

As good of a fighter that MailMarshal is, a small amount of new spam emails will reach the end users. This is an unfortunate and expected side effect of the TRACE team's effort to block as few legitimate emails as possible. It is also due to the ongoing determination of evildoers to develop strains of spam that might evade detection even for just an hour before it is destroyed. To ensure that you are maximizing MailMarshal's spam-fighting capabilities, please see the recommended readings at the end of this article.

Basic: http://www.marshal.com/kb/article.aspx?id=10810

Intermediate: http://www.marshal.com/software/mailmarshal_smtp/ MailMarshal_Anti-Spam_Configuration.pdf

Advanced: http://www.marshal.com/software/mailmarshal_smtp/ MailMarshal_Anti-Spam_Advanced.pdf

M★RSHAL™