

## letters to the editor

### TO ROBERT HASKINS:

I read your article in the August '04 ;login:. I have some comments.

Under your discussion of SPF in the last paragraph, you state, "The real way to fix email is to replace RFC 822 with a more secure protocol." Of course, RFC 822 doesn't specify a protocol, it specifies a message format. Also, as I'm sure you're aware, this protocol has been updated. I think citing RFC 2821 would have been more appropriate.

Parenthetically, I think replacing SMTP is unrealistic. We can't just have a "Flag Day" like this, which means there would have to be "translators" between the old and new protocols. These would continue to pass spam until they all went away. When would they go away? My guess is at about the same rate that SPF would be adopted.

Also, you state that SPF doesn't solve the "spam zombie" problem. It does prevent spam zombies (and anyone else) from forging another's domain without their explicit or implicit consent. I believe this would be a big help.

I also don't see why SPF is more likely to be adopted by the big email hosting providers than the small ones. Small ones probably have more to gain ('cuz they can less afford to be joe jobbed), and it's not that much work. It's less likely to be adopted by very decentralized domains, but that's an issue independent of size. I've published SPF records for a tiny number of email subscribers, and I know I'm not alone.

While SPF is imperfect (you're absolutely correct that email forwarding is problematic), I still believe it's a good step forward. It's designed to stop "joe jobbing," and it can succeed in doing that if listening to SPF records is widely adopted. The uptake on publishing

SPF records can be slow and SPF could still be effective.

Best,

NICK CHRISTENSON  
npc@gangofone.com

### ROBERT HASKINS REPLIES:

You are indeed correct about RFC 822 and RFC 2821. As for my comments on replacing the underlying protocol, of course replacing it is unrealistic. But solving the problem of spam once and for all will require a re-engineering of the SMTP protocol in my (and other people's) opinion. If the rate of spamming keeps increasing at the current pace, we will have no choice but to either throw out the email functionality altogether or do something really drastic like re-engineer the SMTP protocol. Unfortunately, every other anti-spam solution is just a band-aid, and SPF is no exception.

SPF doesn't help the zombie problem directly, but I suppose it does help it indirectly.

As for adoption rates, the providers who host the largest number of mailboxes (and whom the spammers most often use for their joe-job attacks) have the most to gain from SPF. I'm not saying that smaller providers won't have *anything* to gain, just that big providers have *much more* to gain.

As far as SPF record enforcement/listening goes, I think that the MTA/SPF integration needs to get much better before SPF enforcement will be widely adopted. I will admit, I haven't set up an MTA for SPF enforcement. But from a quick perusal of instructions for doing so, it does not look like an easy, straightforward task.

My point wasn't to discount SPF totally but, rather, to provide an attempt at a balanced introduction to SPF. I don't think I achieved my goal!

ROBERT HASKINS  
rhaskins@cnetwork.com