

# Re: increase in spam and what to do about it

---

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2006-11/msg01584.html>

---

- *From:* [bill@xxxxxxxxxxxx](mailto:bill@xxxxxxxxxxxx) (Bill Gunshannon)
  - *Date:* 22 Nov 2006 22:21:25 GMT
- 

In article <1164228129.949473.153320@xx>, davidc@xxxxxxxxxxxx writes:

Bill Gunshannon wrote:

In article <1164209725.524594.74340@xx>, davidc@xxxxxxxxxxxx writes:

Not to mention all the legitimate emails that your server will reject because your potential customer is using an ISP that happens to get itself "blacklisted".

Which is the same set of "potential customers" – I'm just testing the RBL at a different place.

But, if you just change RBL's you open yourself up to all the places the other RBL had that the new one doesn't and your back where you started.

There are technical solutions that can help quite a bit.

As fast as you can come up with a technical solution the spammers will come up with a way around it. It has to be stopped at the source, and there is no technical way of doing that. There is a social way.

SPF is one of the social ways (setting up a trust relationship), but spammers are getting around that, too.

Not sure what SPF is, but I can assure you there is no way for spammers to get around my method.

Re: increase in spam and what to do about it

Both of these can be fixed with my social solution. Right now there is no incentive for any ISP to fix any of this while there are many incentives not to.

Then the social solution (valid or not) is socially unaccepted.

My social solution has not yet been tried, so we don't know that it is socially unaccepted.

The big social problem is that just enough people BUY from these scams to make them profitable enough (even if only the gambling sense – I almost won all my money back, so just one more spam run and I should finally hit to big one!).

Actually, I saw an interview on the news with a commercial spammer. he said all it took was .1% return for him to make a profit. Of course, that leaves the other 99.9% (us) having to deal with it. It will always be profitable for the spammer, which is why it must be stopped at the source. Right now it costs them nothing to send out 100,000,000 emails. The only solution is to remove that conduit so they can't send them.

Unless you charge per e-mail, there's nothing removing the conduit or preventing its abuse. But then you penalize good people just for the sake of banning the bad people.

Metered service has been looked at and it is unacceptable. Plus, it doesn't stop spam but is very likely to make the innocent pay for it.

And yes, the response rates don't have to be big when you can case that wide of a net.

How do you stop it at the source? Which is the spammer, himself?

True. You stop it by not giving the spammer a venue from which to send his spam. The sysadmins all agree (by contract) to not allow spam to be sent from their systems. Penalty: ostracism. The sysadmins of the local mailsystems have AUP's that carry penalties (which depend on the type of

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

organization, ie. ISP – include hefty fines in your customer contract, business – employee can be fired, school – expulsion or other academic sanctions, etc.) Thus, the spammer has no place where he is welcome on the new email network.

Personally, I doubt that the useful base of legitimate mailhosts is "orders of magnitude" larger. The actual number of users has little if any effect on the "trust relationships". It is the admins of the mailhosts themselves that establish the trust. Much like what is done Usenet News today.

Well, given the size of the internet, number of attached companies, it much larger than it was back when I first go my internet connection. What what's to keep a spammer from signing on an ISP and violating that trust, causing other mailhosts to block them?

Read what I said up above. The customers of the ISP all sign a contract (I know I had to!) You put serious penalties in the contract.

Years ago panix, epoch, and many other ISP's played constant whack-a-mole against spammers creating accounts on their networks.

But they have never instituted serious (and enforced) penalties against the people who violate their AUP.

Many of the current RBL's already do this kind of "trust relationship" with known mail hosts, too. We've already done that.

RBL's are an attempt to fix the existing system (and protocol which most people admit is flawed). The "trust relationship" needs to be between the mailhosts and not some third party who has nothing to do with actually transferring email.

But that would be much easier to do today as basicly anyone can talk to anyone, from the technical standpoint. We could have central hubs, like what was done by seismo in the old days, but they would be more

Re: increase in spam and what to do about it

of a convenience than a necessity. I am not saying everyone has to have an explicit agreement with everyone else with whom they wish to exchange email. I am saying that there needs to be an explicit agreement drawn up that everyone who wishes to take part must sign (as a legally binding document) in order to exchange mail with anyone in the Email network. Once you join the network, peering is can be left to the individual admins. Again, much like Usenet News, but with a much stricter and enforceable AUP.

So, how do you get everyone that wants to send email to sign an AUP,

You don't need everyone, only those who want to return email to the useful form it had 20 years ago.

and who do they sign it with?

Whoever they decide they want to use for their email so they don't have to put up with all the spam. This could be their school (we already have an AUP for use of any of the University's computing resources, I to the best of my knowledge, SPAM coming out of here has never been a problem, but I am sure the committee responsible for it would agree to adding an explicit no-spam clause.) Or it could be a remote Email service like Gmail or Yahoo but specifically set up to fill this need.

After all, who would the enforcing body be?

If the users sign a contract, that would be the courts. :-) Especially if the contract includes serious financial penalties.

We have ISP's and providers with AUP's today.

Name one ISP that has an AUP that includes a serious fine for spamming!

Usenet news isn't good example, since it's been rampant with spam even before e-mail (remember the Brierbart Index and Cancelmoose? Canter and Seigel?).

I didn't mean it as an example of a system that works perfectly, I meant it as an example of a system that only works between "trusted hosts".

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

Try setting up a news server on your own. It won't go very far until you find at least one other News site willing to exchange with you. There is really nothing to stop these "trusted hosts" from having stricter AUP's so that none of the above existed. As a matter of fact, I believe that was the intent of USENET-II (I haven't looked lately to see how this has worked out.)

If only it were so. While much of the spam coming into my mailserver comes from the proverbial "rogue" PC I get a considerable amount from ISP's who really have no problem with spammers. The profit currently outweighs the potential cost.

True, but those ISP's can be (and likely are) RBL'd against.

If they were, I wouldn't be getting the spam. :-)

Even early in the battle with Walt Rines and Sanford Wallace, there was substantial blackholing of the entire AGIS backbone (a very strong social statement) against spam and their support to two of the worst known offenders.

And who paid the price? What effect did this have on AGIS legitimate users?

Wasn't pretty. But that was the "social solution" at the time. Since people didn't know where they would appear on AGIS networks, more and more places blackholed all AGIS networks. AGIS eventually was forced to drop them, and they then promised to create the "SPAM-bone" so they could run all the spam on it they wanted. Getting peers proved to be problematic.

Sorry, ISP's don't see it that way. It's all about the money. As long as there is money in spam they will support the 0.1%.

Sometimes it's not the money, but the expense. Chasing and terminating spammers takes time and effort. Then they just get a new account or you end up with a new batch. Eventually, it just cost less to ignore it.

Re: increase in spam and what to do about it

Unless you made them sign a contract in the first place that had severe financial penalties.

There are some major ISP's that show up on RBL's and do nothing to get back off them. Why? Because there are still lots of email servers that don't use RBL's or can't because of the very reason you cite above. That leaves lots of potential targets and, anyway, as long as the spammers are willing to pay for the connection and service, why would the ISP care if the email ever gets delivered?

But they typically do. That's why far fewer SMTP servers allow relays anymore, and the defaults are now to NOT relay. I.e. sendmail has been that way for many years now. And some of the older RFC allow relay tricks are now disabled, such as the percent-hack.

That doesn't mean they can't identify and isolate that 0.1%, but the problem is getting harder and more frequently occurring than ever before (i.e. the new SpamThru trojan).

Which comes back to why it has to be stopped at the point of origin. And we won't even get into the load on the whole infrastructure of rejecting at the destination rather than stopping it at the source.

But how do you reject it at the source? You get a customer to sign an AUP? As I mentioned, we've already gone through that whack-a-mole tactic of dealing with spammers years ago.

But the AUP's they signed in most cases included no penalty beyond losing your account. They need to carry serious financial penalties as money is all anyone understand today.

And why is that? Because right now, under the current system there is no penalty for allowing it and a perceived penalty for stopping it.

Re: increase in spam and what to do about it

Exactly – if a spammer spams through your mail server, and it gets blocks (i.e. you socially disagree to accept their email traffic), all your customers are punished. Not good for your business. You can't stay in business when you treat all your customers like crooks.

Under my system, one would assume that the peers would not need to be so draconian as to cut someone off on the first incident. Of course, it would likely depend on how the originating site handled the incident. If they had in their AUP (agreed to as a contract so that the courts are an arbiter) something along the lines of a \$1000 fine for each incident of SPAM sent by the customer and they enforced it, it would be very un-profitable to end spam and there would be little if any chance of not getting caught. Thus removing the greatest incentive to spamming.

I don't agree on two points. I don't believe that "The technical ability to zombie a box has got to be eliminated/reduced". And, moreover, I don't believe that "The technical ability to zombie a box can be eliminated/reduced".

No, it has to be. There is just too much damage via phishing, identity theft, DDoS, and more to allow hundreds of thousands of Billy boxes on the network. The cost is too high, and currently Microsoft does not have the pressure to substantially fix it, despite the financial loss caused by zombied machines. Either they need to be hardened or more isolated. Maybe Microsoft can't do it, but eventually some government or business is going to take a huge loss (probably a lawsuit) due to damage caused by one or more Windows boxes.

Sorry, but I don't believe this will happen until MS runs its course and is supplanted by something better.

Eventually, someone is going to get an identity theft class-action lawsuit against a company, and will win because they can demonstrate that the data on their Windows boxes was exploited because they either didn't update their virus definitions enough, or missed a service pack.

But you just gave the best defense. The user "didn't update their virus definitions enough, or missed a service pack" and thus, it was their own fault.

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

I just want the utility of email that I had in the original Usenet days back.

And frankly, I was around in the old Usenet days, too, but I never signed an AUP to prevent me from spamming or any such thing.

What's your point? Back in those days there were machines on the DARPA NET that didn't even have passwords. Society in general was different and among the computer community in particular. Draconian AUP's weren't needed. Of course, people also used to leave their cars and even their houses unlocked, too. I can't think of many who still do.

Email was just a poor medium to spam, so it wasn't used that way. Your "original Usenet days" weren't socially or technically better than before, just not viewed as a target of abuse.

I disagree. I think they were better socially. The lack of Spam was probably more due to the limited social coverage nature of the medium.

Usenet News was where the spamming problem started due to its more "broadcast" nature. E-mail didn't become prevalent until the middle 1990's once the Internet started to gain mindshare and more people had e-mail (CompuServe, Prodigy, AOL).

There were lots of different Email systems in the past, USENET, FIDO, Bitnet, etc. And then there were the commercial services like you mention, although Prodigy and AOL were latecomers. there was TELENET and TYMNET. But what was lacking technically was the computing resources and the conduit to handle the volume needed for spamming.

Your sysadmin choice of social "trusts" have been implemented by public and private RBL lists, spamassassin, Bayesian and other filtering methods, but most can't just whitelist the rest of the world, either, since many people NEED to be contacted by previously unknown places (i.e. me). And until you get that first spam (or subscribe to an RBL or other service to look at it for you), you really can't tell if it's spam yet.

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

As I said, RBL's is not a trusted host relationship it is trying to put the responsibility on a third party and after the fact. That is a system destined to fail. It must be stopped at the point of origin and before the fact. It must be proactive and not reactive in order to work. If it is reactive, there are just too many potential spammers to deal with.

But as the whack-a-moles at ISP's worked (socially terminating their connectivity for AUP violations),

More aggressive penalties are needed in the AUP!!

spammers just used different tricks,  
like third party SMTP relays,

You don't relay. Oh, and did I mention that my proposal doesn't use SMTP. :-)

exploitation of WinGate firewalls,

Not sure what that means, but I'll bet it relies on SMTP to send the mail from the attacked machine. See above.

exploitation of formmail.pl scripts

Well, I won't even go into the potential security problems with any PERL or PHP scripts, but I can tell you that I was able to win the battle here to not allow the mail function on our web server.

(which I have a spammer attempting to do that off the Hobbyist web form for the past few days – topcopl2@xxxxxxx), abuse of SOCKS4 proxies, and the growing tide of bot-nets.

I'll bet all of these depend on SMTP as the underlying protocol and they also don't care who connects.

Re: increase in spam and what to do about it

And forget just e-mail, IM spamming and web forum/blog spamming is on the increase, too.

They were never truly useful anyway, so I really don't care. I am trying to salvage Email, let someone who cares fix the others.

The problem is whatever the social contracts are, the spammers will violate them and bypass them, as they have for years. Spammers have been fined, sued, terminated, blocked, and more (which is about as strong of a social solution statement you can make), yet they still persist.

Sorry, I have never heard of any spammer who has been held financially liable for his actions. Please provide some real examples.

There is no one solution. There may not be a solution. But you also can't turn back the clock to the good ole days, either. Profiteers will try anything they can to exploit the system for a measly buck.

Or we can just sit here and let the bastards win. Sorry, I would rather try to convince people in a position to do something that the time is ripe for fixing things.

bill

—

Bill Gunshannon | de-moc-ra-cy (di mok' ra see) n. Three wolves  
bill@xxxxxxxxxxxxxxxx | and a sheep voting on what's for dinner.  
University of Scranton |  
Scranton, Pennsylvania | #include <std disclaimer.h>

.