Unsolicited commercial – and usually fraudulent – e-mail (spam) is a constant headache for individual users and for mail-server administrators. In this second part of a three part series, I look at why we are suffering from this plague.

At the deepest level, spam is a result of the fundamental flaws in the TCP/IP protocol suite. The original design never envisaged a need for security; no one in the 1960s and 1970s imagined that the entire world would become dependent upon Internet functions to carry out normal business communications and services. IPv4 simply has no inherent provisions for strong identification and authentication of the origin of packets: anyone can spoof the originating address of a packet and evade the consequences of their fraud. Consequently, criminals routinely create waves of falsified packets using open mail relays or machines commandeered to create botnets. Therefore, one possible contribution – not solution – to reducing the spam problem will be increasing use of IPv6, which does have provisions for incorporation of verifiable authenticators of identity for the originating servers sending out packets. Simply being able to track down the origin of a particular stream of spam will help by supporting a concerted program to identify and correct poorly secured SMTP servers.


- About four fifths of the respondents were taking measures to block spam
- About half of all respondents claimed never to have opened spam e-mail
- Almost all respondents said that if they recognized e-mail as spam, they deleted it at once
- About four fifths of the respondent said that they were aware of malware threats but only one fifth said it was very likely that their computers would be infected
- When asked about the likelihood of infection by bots, “14% of consumers believe they will never be infected by a bot; 41% think it is not very probable; and 37% describe themselves as neutral”
- About one sixth of the non-expert respondents admitted to responding to offers received in spam.

To what degree should we hold the owners and users of systems so poorly secured that they have become part of a botnet? One position is that it is absolutely not the fault of the victims that criminals have subverted their resources. Why blame the victims? Wouldn’t holding them responsible be morally indefensible?

Not necessarily.

In the last of this three-part series, I’ll examine some possible ways of improving our defensive position against spam.

Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.