

## Re: Best way to enable logs to catch a suspicious spammer inside org

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0537.html>

---

**From:** Herb Martin (*news\_at\_LearnQuick.com*)

**Date:** 12/28/04

Date: Mon, 27 Dec 2004 23:42:40 -0600

> > *First, how do you know this?*

>

> ==>*Reported by two independent agencies that spam is being generated from*

*a*

> *workstation in my domain. I see the headers of such spam mail and because*

> *the claim coincided with an workstation IP range in which SMTP is allowed*

> *for such subnet and because I had problems with users from same subnet in*

> *the past, I think the report is somewhat credible and I would like to*

> *investigate this.*

You should see a pattern — we both wanted to know how you knew the IP was invalid (which is really not the case as far as we can tell from your report otherwise.)

How many machines do you physically have in that subnet?