Proposal: Block known residential address blocks from directly submitting mail to SMTP.UCLA.EDU

Summary

Much of the spam and viruses received by campus users is generated or relayed by infected and/or compromised personal computers. In almost all cases, these computers utilize the services of corporate or commercial e-mail servers for the purposes of sending and receiving mail. There is no reason, outside of compromise of infection, for these machines to directly submit mail to SMTP.UCLA.EDU. Refusing to accept mail from these hosts should drastically reduce the amount of spam and viruses that are processed by campus mail servers and delivered to users’ mailboxes.

Current practice

SMTP.UCLA.EDU accepts inbound mail for UCLA e-mail addresses from any external IP address. Internally, access is blocked from the Residential Program network, dial-up users, and public workstations in the Library.

Proposed practice

Refuse to accept mail from network address blocks known to be residential services such as dial-up modems, DSL lines, and cable modems.

Costs

Subscribing to a listing of dial-up/DSL/cable address blocks has been quoted at $11,000 per year.

Impact

Blocking residential sources from accessing the SMTP.UCLA.EDU cluster will increase the useful lifetime of these servers, and slow the cluster’s rate of growth. Performance levels will improve as fewer bounce notifications are processed.

Valid e-mail sources could be blocked. Exceptions could be made to allow trusted sources to bypass the blocks if necessary.

While not directly measurable, staff productivity should improve from the decrease in spam, and fewer server resources will be required to store spam.