CNS /Update Newsletter Feature

New OIT Standard: Authorized E-mail

CNS Document ID: u040104a
Last Updated: 1/01/04

UF Information Technology

UFIT
2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

New OIT Standard: Authorized E-mail ................................................................. 3
New OIT Standard: Authorized E-mail

Did you know that your workstation can be used by spammers to actually send spam out? Recently spammers have been abusing end-user workstations; previously they targeted mostly servers and open relays. Vigilant administrators have been cutting the number of vulnerable machines, so spammers have a large number of new sources (your computer!) from which they send illicit traffic.

Industry standards and best practices indicate that SMTP (Simple Mail Transfer Protocol) filtering and SMTP AUTH (for "authentication") are commonly accepted, and expected, security practices. UF's security team has recommended a plan, authored by Network Security Engineer Jordan Wiens, to implement these standards.

The plan is to first filter mail traffic from nomadic (e.g., wireless and dial-up) users destined off-campus so it must come through registered campus mail servers, and then to enable SMTP AUTH for that population. This will further restrict traffic so that nomadic populations must use the main campus mail server (smtp.ufl.edu). Forcing authentication allows more precise access restrictions. Users can be prevented from inadvertently sending spam (if they are abused by a malicious spammer), while still being allowed access to other network resources. Eventually all mail from campus outbound will be restricted to authorized mail servers, not just mail from nomadic populations.

Most people in the university community probably already use the campus mail server. If your mail client doesn't already use a registered mail server, you should make this change soon. If you use a departmental mail server, you need not worry. If you're not sure, contact Network Services at net-services@ufl.edu [mailto:net-services@ufl.edu].

Filtering outbound traffic and requiring SMTP AUTH are potentially large changes that will affect nearly every user on campus. For this reason, a protracted timeline is suggested to allow a smooth transition and resolution of any potential issues.

- Ongoing - Begin registration of campus mail servers
- February 17, 2004 - Restrict nomadic populations (dial up and wireless) from any off-campus mail servers
- March 16, 2004 - Enable SMTP AUTH for nomadic populations on main campus SMTP server
- March 16, 2004 - Restrict nomadic populations to smtp.ufl.edu for outbound mail
- April 13, 2004 - Require SMTP AUTH for nomadic populations on main campus SMTP server
- May 18, 2004 - Restrict outbound mail traffic to registered campus mail servers

Administrators should coordinate with the campus Help Desk to educate users about these important changes. For more information, see http://net-services.ufl.edu/security/admins/email-std.shtml.
These changes will allow for more secure transmission, better accountability, and a reduced impact of virus and trojan-infected users on campus.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>