CNS /Update Newsletter Feature

Virus Scanning Successful!

CNS Document ID: u020301a
Last Updated: 2/20/02

UF Information Technology

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

Virus Scanning Successful! .......................................................................................3
A Day in the Life of the Virus Scanner ....................................................................3
Virus Scanning Successful!

In order to help rid UF's GatorLink service of inbox-clogging viruses, NERDC is now scanning mail that goes through GatorLink's smtp.ufl.edu server.

"We originally undertook the task of virus scanning while trying to defend ourselves from the SirCam virus. Many GatorLink mailboxes filled up in a matter of hours-just from random virus traffic. After they would fill, the user couldn't get any more legitimate e-mail, and new messages for them would just fill up one of the mail queues," said Steve Ulmer, manager of the Open Systems Group at NERDC.

When scanning was first implemented, Ulmer said, 25 percent of the e-mails were infected. "We're now seeing a steady decline, but we don't yet know what the average 'virus background noise' will be."

The scanning helps raise the UF computing community's awareness about viruses.

"Many people may not even realize that they're infected and sending out infected messages every time they connect to the Internet. Now, they're getting rejection messages from their mail programs, so hopefully they'll recognize the problem, or maybe call the help desk who will recognize the problem," Ulmer said.

The response from departments has been very positive too. "Scanning every message is expensive, but the response this service has received makes it clear that there was a large demand for something like this. I've been contacted by a few departmental administrators, indicating that they will now not have to spend money earmarked for locally implemented virus scanning on their e-mail servers," he said.

Even though we are scanning the messages that go out of smtp.ufl.edu, scanning should still take place on people's desktop computers. "We don't clean the viruses, so if there's a virus infecting an item you need (such as a Word document or a spreadsheet), then you'll have to clean it yourself," Ulmer said. Also, this scanning does not touch every piece of e-mail that goes in or out of campus. "Not all mail transits this server, though. Only outgoing messages from user e-mail programs that are configured to use smtp.ufl.edu or incoming messages to @ufl.edu domain addresses are scanned," he said.

A Day in the Life of the Virus Scanner

Tuesday, January 23, 2002

255,999 messages received and processed

105,322 additional messages from prodigy.net.mx rejected*

51,275 additional messages rejected due to origin or relaying

25,927 contained viruses which were wrapped and sent to recipient

25,672 messages with viruses discarded

*prodigy.net.mx was blocked because the SirCam virus uses that as its default "from" domain.
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>