"Richard Reeder"
<rreeder@NOTES.CC.SUNYSB.EDU>

02/27/2004 04:34 PM

To "Torre,F.Jason" <FTORRE@NOTES.CC.SUNYSB.EDU>

cc

bcc

Subject Email, Computer viruses, and Spam

To: All Faculty and Staff

In the last six months, the campus has experienced a ten fold increase in the number of email viruses being sent to campus users. To combat the spread of viruses and reduce Spam, DoIT has taken the following steps for users of our email servers (Please note that if you use a non-DoIT server for your mail services, some of these protections do not apply.):

o All in-bound email to DoIT servers is scanned for known viruses and those messages that contain infected attachments are deleted.

o Attachments in emails containing the following file extensions will be removed from the message: .scr, .vbs, .pif, and .exe. Users will still get the email minus the attachment with an explanation that the attachment has been removed because it violates the content filtering rule (i.e. contains one of the prohibited file extensions).

o A real-time Intrusion Protection System has been installed at the border of the campus Internet and Internet2 networks. This device is programmed to look for both email and other traffic that contain viruses in their payload. If found, the packets are not delivered to the user.

o DoIT has acquired software to detect Spam and is currently tagging those messages by including 'SpamAlert' in the subject of the message. For Notes 6.5 users, please refer to http://clientsupport.cc.stonybrook.edu/notes/SpamAlertRule.shtml for instructions on creating mail rules that can automatically move these messages into your 'SPAM' folder.

While these steps have helped to reduce vulnerability to virus infection, they have not completely eliminated it. To further reduce risk of infection, campus users must play an important role. Here are some suggestions that will help reduce your risk of being infected:

o Ensure that you have the campus site-licensed Symantec (Norton) AntiVirus installed on all your Windows machines and your virus signature files are kept up-to-date. To check the setting of your antivirus program, Click on Start, Programs, Symantec Client Security - Symantec AntiVirus Client to display the AntiVirus Status page. Check the last item on the bottom right. If the Virus Signature file is not within the last 7 days click on the Live Update button and follow the instructions. If the Live Update button is greyed out your on campus desktop, then the program is managed by the Server in the Parent Server field. You do not have to worry about updating the virus signatures.

o As a rule, always treat email attachments with caution. Because mass-mailer viruses, such as Bagle, hijack email accounts and send messages to known contacts, viruses can initially appear to be legitimate messages. If you cannot confirm with the sender that a message is valid and that the attachment is safe, delete the message immediately. In addition, regardless of the sender, you should never launch an attachment that has the following file extensions: .exe, .com, .vbs, .scr, and .pif. These file types are known to be used to transmit viruses.

o Be aware that the "From:" field in an email message is easily spoofed. If you receive a suspicious message from someone that you know, do not launch any attachments without confirming the identity of the sender.
Do not forward an email message that you suspect contains a virus to other users. You may either delete the message or send it to virusalert@notes.cc.sunysb.edu .

o Do not follow instructions to delete files contained in an email message, especially if the message appears to come from a vendor (e.g. Microsoft) These hoax emails typically ask you to follow their instructions, including deleting of specific files on your computer and then ask you to forward the message to everyone that you know. If in doubt forward the message only to virusalert@notes.cc.sunysb.edu .

o Be aware that Microsoft and other vendors never distribute software or ask for personal information by email.

DoIT is continually striving to provide a safe and efficient computing and networking environment. The Division hopes that you can assist us in doing your part to reduce the spread of viruses. Thanks in advance for your anticipated cooperation.

Richard W. Reeder
CIO
Stony Brook University
State University of New York
631-632-9085 Voice
631-632-2160 FAX