



February 14, 2003

OKLAHOMA BULLETIN NO. OK270-3-4

SUBJECT: IRM - Email Security

Purpose: To remind employees of the need to be alert to the possibility of viruses in email attachments and malicious web links.

Expiration Date: September 30, 2003

Email attachments and malicious web sites containing viruses pose a significant threat to the security of USDA computers. Opening an infected attachment or a malicious web link can cause corruption or deletion of the operating system and data on the workstation and on the server. A virus may transmit itself to additional systems either through the network or through the use of automatic mailings to entries in address books.

In most instances the only recourse once a system has been infected is a lengthy process to reformat the hard drive, reload all software and attempt to restore any data from a backup made prior to the infection.

Even though software on our mail servers attempts to filter out messages containing such attachments and the McAfee anti-virus software is being automatically updated neither of these programs can provide 100% protection. It remains the responsibility of users to always be alert to the contents of messages and the names of attachments.

Users should never click on an enclosed link contained in an email if the sender of the message is not someone you know - especially if the link is to a system outside the United States.

Users should never open an attachment to an email message when the attachment name ends in one of the following extensions:

**.COM .EXE .BAT .LNK .PIF .VBS .REG .VBE
.WSH .WSF .JS .JSE .JSF .SHS .CHM .SCR**

Even if the sender of the message is someone you know and normally communicate with don't open the attachment. Delete the message and immediately delete it from the Netscape 'Trash' folder.

In the event that a suspect link is accessed or an attachment with one of the listed extensions is opened, immediately notify the IT staff at the State Office for guidance. Just because there wasn't any immediate noticeable action by a virus when the attachment was accessed does not mean everything is all right since some viruses have built-in delays.

Please print this bulletin and post it near all workstations as a reminder while reading your email.

/s/

M. DARREL DOMINICK
State Conservationist