

Safe Computing Initiative - Virus

Virus infections have caused millions of dollars of damage to computer networks over the past few years. The arrival of the Internet allowed these viruses to spread faster and inflict greater damage. Virus writers have used “social engineering” techniques to trick computer users into installing viruses onto computers. The products to combat these viruses have matured and are now widely installed. Yet viruses still spread because of social engineering tricks and software vulnerabilities that have not been “patched.”

DANGERS OF VIRUS INFECTIONS

Every virus carries its own “payload.” Some are intended to damage files or programs (e.g. Macro Viruses and the anti-exe virus). Some are intended to damage hardware/Kill computers (e.g. the Chernobyl virus). Others are intended to crash computer networks and clog e-mail servers (e.g. the Code Red virus). Recovering from a virus infection is a time consuming and costly process and diverts technology resources away from supporting instruction in the school system.

SOURCES OF VIRUS INFECTIONS

The Internet is the most common avenue for viruses to spread. Classic viruses require action by the computer user in order to be installed on a computer. The general method for this type of virus is to arrive as an e-mail attachment. The virus then attempts to trick the computer user into opening the “document” so the virus may be installed. A less common spreading method is for a virus to reside on a web page or in a “pop up window.” When the computer user clicks on the web page the virus installs itself on the computer.

The newer “Worm” viruses spread automatically by repeatedly exploiting vulnerabilities in software (operating systems such as Windows 98 or 2000).

REQUIRED ACTIONS

Because of the dangers presented by viruses and its diversion of resources away from instructional issues, specific actions need to be taken that include:

STAFF

1. Staff should not open e-mail attachments from unknown senders.
2. Staff should open e-mail attachments from known senders with caution
3. Staff should verify that anti-virus software is running on the computer they use.
4. Staff should continue to exercise due diligence when visiting web sites. Many malicious sites open Pop-Up windows which may trick you to download/install viruses.

TECHNOLOGY DEPARTMENT

5. Anti-Virus software should be installed at the Firewall or Mail Server level.
6. Anti-Virus software should be installed on every server and every workstation.
7. E-mail with dangerous attachments should not be delivered to user mailboxes.
8. The network firewall should not permit viruses to spread outside our network.
9. Software vulnerabilities should be fixed with released software patches.
10. Software that has known vulnerabilities but is not “patchable” should no longer be used.

SUMMARY

In order to safeguard our network from the threats presented by virus infections Radford City School employees should be very cautious when opening e-mail attachments and continue practicing safe computing habits.

