

Date: Thu, 12 Mar 1998 09:57:32 -0600
From: Meredith Brown <racer@lanl.gov>
Subject: Blue Alert: Computer Virus Hoaxes

Project Hanford Lessons Learned

Title: **Computer Virus Hoaxes**
Date: February 25, 1998
Identifier: 1998-RL-HNF-0009

Lessons Learned Statement:

E-mail messages warning of computer viruses should NOT be forwarded to anyone except your computer security contact. Many virus alerts are actually hoaxes that, when perpetuated, absorb more time to deal with than do real viruses.

Discussion of Activities:

Summary:

Interspersed among real computer virus notices are many hoaxes. While these hoaxes do not infect systems, they are still time consuming and costly to handle. The DOE Computer Incident Advisory Capability (CIAC) office spends more time de-bunking hoaxes than handling real virus incidents.

Details:

A recent flurry of computer virus hoaxes indicates that many computer users can not distinguish between a valid virus warning and a hoax. Most successful virus hoaxes include (1) technical sounding language, and (2) credibility by association.

(1) If the warning uses the proper technical jargon, most individuals, including technologically savvy individuals, tend to believe the warning is real. For example, the Good Times hoax says that "....if the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop which can severely damage the processor.....". The first time you read this, it sounds like it must be something real. With a little research, you find that there is no such thing as an nth-complexity infinite binary loop and that processors are designed to run loops for weeks at a time without damage.

(2) "Credibility by association" is referring to who sent the warning. If the janitor at a large technological organization sends a warning to someone outside of that organization, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real. If a manager at the company sends the warning, the message is doubly backed by the company's and the manager's reputations.

Individuals should also be especially alert if the warning urges you to pass it on to your friends. This should raise a red flag that the warning may be a hoax. Another flag to watch for is when the warning indicates that it is a Federal Communication Commission (FCC) warning.

According to the FCC, they have not and never will disseminate warnings on viruses. It is not a function of their organization.

Another area of concern is Internet chain letters that may or may not be true. For more information on Internet chain letters, refer to <http://ciac.llnl.gov/ciac/CIACChainLetters.html>.

Analysis: N/A

Recommended Actions:

If you receive a virus warning message via E-mail, DO NOT FORWARD THE UNCONFIRMED WARNING to other employees. Instead, report the message to the your Computer Protection Program Manager (CPPM) for validation. The PHMC CPPM can be reached at 376-0237. If the warning turns out to be a valid concern the CPPM will ensure that employees are notified as appropriate.

Estimated Savings/Cost Avoidance (if applicable): N/A

Priority Descriptor: BLUE/Information

Functional Categories (DOE): Information Technology, Safeguards & Security

Functional Categories (User-defined): N/A Originator: Fluor Daniel Hanford, Inc.

Contact: John Bickford (509) 373-7664, FAX: 376-5243 email:

[Lessons Learned Sitewide@rl.gov](mailto:Lessons_Learned_Sitewide@rl.gov)

Authorized Derivative Classifier: Dave Briggs 372-3343

Reviewing Official: John Bickford, 373-7664

Keywords: computer hoax, computer virus, computer security, computer warning

References: CIAC Internet Hoaxes (<http://ciac.llnl.gov/ciac/CIACHoaxes.html>) Computer Virus

Myths home page (<http://www.kumite.com/myths/>)