

Date: Mon, 08 Feb 1999 16:15:20 -0600
From: Meredith Brown <racer@lanl.gov>
Subject: Blue Alert: Common Internet Hoaxes

Project Hanford Lessons Learned

Title: Common Internet Hoaxes

Date: January 19, 1999
Identifier: 1999-RL-HNF-0002

Lessons Learned Statement: Many questionable email warnings are hoaxes and should NOT be forwarded. If the warning seems strange, validate it with your computer security manager or other authority. They will take action to warn others as appropriate. You should not forward any such messages. Email 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: A recent flurry of hoaxes indicates that many individuals can not distinguish between a valid warning and a hoax. If there is any question about the authenticity of the warning, do not circulate it to others. If you receive an unvalidated warning, pass it to your computer security manager or other authority to validate. The following summary of recent messages illustrate the variety of Internet hoaxes currently making the rounds:

* If you are driving after dark and see an on-coming car with no headlights turned on, do not flash your lights. This is common gang initiation ritual that requires the initiate to drive with his lights off. The first oncoming car to flash its lights becomes the target for the new gang member to shoot at or into.

* Drug users are using coin return slots in public telephones to hide or dispose of their needles. When people try to recover returned coins, they are stuck by these needles and infected with various diseases.

* A telephone caller identifies himself as an AT&T Service Technician conducting a test and requests the victim press nine (9), zero (0) and the pound sign (#) to complete the test. This action gives the requesting individual access to your telephone line, allowing them to place long distance telephone calls billed to your telephone number. (NOTE: GTE and AT&T representatives say that this may actually work for some telephone systems in large offices but NOT on the Hanford Site.)

* Join The Crew, Penpal Greetings, Bud Frogs Screen Saver, Win A Holiday, and other Internet hoaxes involving false virus warnings, are constantly circulating on the Internet. For more information on Internet hoaxes, refer to <http://ciac.llnl.gov/ciac/CIACHoaxes.html>.

Analysis: There are several methods for identifying hoaxes. Two factors make a successful hoax: (1) technical sounding language and, (2) credibility by association. 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. Upon receiving a warning, see if it includes the name of the person originally submitting it. Contact that person to see if he/she really wrote the warning and really experienced the event. Warnings without the name of the person sending the original notice or warnings with names, addresses and phone numbers that do not actually exist are probably hoaxes. If he/she is passing on a rumor, if the address of the person does not exist, or if there is any questions about the authenticity or the warning, do not circulate it to others. Instead, send the warning to your computer security manager or your incident response team and let them validate it. When in doubt, do not forward the message.

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>.

Contrary to popular opinion, electronic mail is not free. The infrastructure required for an email system is expensive. Hoax messages load down networks unnecessarily as well as consume time of senders and recipients.

Recommended actions: If you receive an email message with the characteristics described above, DO NOT FORWARD THE UNCONFIRMED WARNING to other employees. Instead, report the message to your manager or security department for validation. If the warning turns out to be valid, then appropriate authorities will notify employees.

Priority Descriptor: BLUE/Information

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

Functional Categories (Hanford specific): None

Originator: Fluor Daniel Hanford, Inc. Submitted by Sandy McInturff of HEHF.

Contact: Project Hanford Lessons Learned Coordinator; (509) 373-7664; FAX 373-2084; email:

PHMC_Lessons_Learned@rl.gov

Authorized Derivative Classifier: Mike Spracklen (509) 376-3730

Reviewing Official: John Bickford

Keyword(s): hoax, security, Internet warning

References: CIAC Internet Hoaxes (<http://ciac.llnl.gov/ciac/CIACHoaxes.html>) and Lessons Learned 1998-RL-FDH-0009