FCC Computer Security Notice

COMPUTER SECURITY WEEK 2002

SPOTTING E-MAIL HOAXES AND SCAMS

Are you a Nigerian Government contracting millionaire, or maybe you're an oil tycoon? Perhaps you are afraid to travel for fear of losing your kidney? These, like other e-mails, are hoaxes, scams and other urban legends. For many years, computer virus hoaxes have been circulating the Internet. In October of 1988, one of the first virus hoaxes publicized was the 2400 baud modem virus. Since that time, these expensive nuisances have flooded the Internet. It is the paranoia of getting a virus that often fuels virus hoaxes.

Internet hoaxes and chain letters are e-mail messages written with one purpose: to be sent to everyone you know. The messages they contain are usually untrue. Most of the hoax messages play on your need to be kind to others. Despite the abundance of them in your inbox, there is a way to identify if they are in fact hoaxes.

How to Recognize a Hoax. If it is too good to be true, it probably is. Most hoaxes come from mass mailers that are unknown and untraceable. Attempts to gain additional information about the offers may result in unknown websites, bogus companies and various other schemes. When phone numbers are present, they should never be called since you may connect to numbers that charge 500 US dollars a minute.

There are several websites that list detailed information about e-mail hoaxes. There are three listed in our additional information section below.

If you do not find the warning at the hoax website, it may just mean that this particular hoax has not yet been reported. See if the warning includes the name of the person sending the original warning. If it does, see if you can determine if the person really exists. If they do, don't send them an e-mail message.

If you still cannot determine if a message is real or a hoax, you should consult your Internet Service Provider, if received at home, or your incident response team, here at the FCC, and let them validate it.

Preventing the Spread of E-mail Hoaxes. FCC users are requested not to spread e-mail messages that are chain letters or hoaxes. Probably the biggest risk for hoax messages is their ability to multiply and potentially cause denial of service. Many people willfully or inadvertently send hoax messages to everyone in their address books.

Spammers (bulk mailers of unsolicited mailers) often harvest e-mail addresses from hoaxes and chain letters. It is also rumored that spammers are deliberately starting hoaxes and chain letters to gather e-mail addresses.

In all cases, do not reply to the messages. Instead, delete them immediately. The FCC Computer Security Officer recommends that this type of mail be handled like Spam. ***Do not forward it. Do not respond to it. Delete it.***

COMPUTER SECURITY TIP OF THE WEEK:

IT IS COMPUTER SECURITY WEEK HERE AT THE COMMISSION. KEEP AN EYE OUT FOR COMPUTER SECURITY WEEK EVENTS ON THE NEWLY DESIGNED CSP WEBSITE.

YOU CAN REFERENCE ADDITIONAL INFORMATION ABOUT E-MAIL HOAXES AT:

- F-Secure Home Page: http://www.f-secure.com/virus-info/hoax/
- MacAfee Hoax Website: http://vil.mcafee.com/hoax.asp
- Symantec Security Response-Hoax Page: http://www.symantec.com/avcenter/hoax.html