

*San Francisco Daily Journal, 10/17/02, p. 12.
Posted with permission of the Daily Journal.
This file cannot be downloaded from this page.*

Don't Delete This Article!!!: Dealing With Net Virus and E-Mail Hoaxes

*Paula Lichtenberg, Librarian
Keker & Van Nest LLP*

URGENT!!!! I'm not sure if this is true, but I'm sending it just in case . . . I wanted to warn you... A friend of a friend was dating a guy from Afghanistan.... He warned her not to go to the mall on Halloween or drink Pepsi or Coke after a certain date...Be careful of used needles drug users have left in coin-return slots in public phones or in movie theater seats It could erase everything on your hard drive.... Pass this along to everyone in your Internet address book.

Along with the spam and other junk mail clogging our Inboxes, we are getting e-mails that forward virus alerts and chain letters and urban legends. Although most of such warnings are in fact hoaxes, not all of them are. You don't want to throw the baby out with the bathwater and ignore valid warnings about worms and viruses that can impact your computer. Not only can these messages be annoying and time consuming to deal with, but now some spammers have developed the capacity to harvest addresses from hoaxes and chain letters, so forwarding the e-mail may lead to lots more spam.

What to Look for When You Get a Virus Alert

There are plenty of real viruses running around, so you shouldn't just ignore a warning out of hand. But not all notices are equal and you should consider:

- 1) What is the source of the alert? Take seriously a warning from a reliable source, such as your IT department, but bells should go off when it comes from an unknown source, or from your uncle, who is forwarding it from a friend, who heard about it from her dentist...
- 2) Does the warning urge you to forward the mail to everyone you know? Genuine virus alerts don't ask you to do this.
- 3) Does the warning give you detailed instructions on downloading a program or deleting files to deal with the virus? A real warning will offer a link to a reputable source for more information.

Dealing With Viruses

Merely reading an email cannot infect your computer. What you don't want to do is open an infected file, which usually will come in the form of an attachment. (But be aware that MS Word documents and other MS Office files, like Excel or Power Point, contain programs that are activated when you open them and they can pass along viruses.)

- 1) Use an anti-virus software and keep it up to date.

- 2) Do not forward the message. The quickest and safest thing to do is simply delete it. If you have concerns about a particular message, look it up on a legitimate web site (see some examples below) or forward it to your IT department to check.
- 3) If you don't know the sender of the e-mail, it is good practice to delete it without opening it.
- 4) Most viruses are found in executable files. If you unexpectedly get a file that ends in .exe or .vbs, the safest thing to do is to delete it without opening it. If you are expecting an executable file, be sure to virus scan it before opening it.
- 5) Don't delete files per instructions in an e-mail without checking first with a reliable source. You may find yourself spending a lot more time re-downloading perfectly safe programs.
- 6) Make sure your Internet browser is updated with the latest security patches from the vendor.

Spotting the E-Mail Hoax

The best weapon against chain letters and other e-mail hoaxes is a healthy dose of skepticism. Some common signs to look out for:

- 1) The message tells you to mail it to everyone you know.
- 2) It doesn't have any contact information for you to check the legitimacy of the mail.
- 3) Phrases like "This is not a hoax" or "This really happened" are usually signs of just the opposite. Using ALL CAPS and lots of explanation points are popular methods of grabbing your ATTENTION!!!!
- 4) The message is supposedly giving you important information ("beware of the Good Samaritan killer stalking women at malls"), but you've never heard anything about it from any other source.
- 5) There really is no such thing as a free lunch. Beware of giveaways of free clothing, cars, gift certificates, cases of Coke. Bill Gates will not give you \$1000 if you forward his message.

Dealing With E-Mail Hoaxes

- 1) Check a web site that debunks hoaxes. Chances are the annoying message you received has been making the rounds and you'll find it on one of the many such sites, such as Urban Legends Reference Pages.
- 2) Don't pass it along. Your delete button is your friend.
- 3) Educate the senders of the messages. Explaining the issues to repeat senders will likely cut way down on the number of false messages you get. At work, an article in the firm newsletter or on your intranet could help educate the staff.

Debunking Hoaxes - Sites to Check:

There are lots of good sites out there. Here are a few I like:

- 1) Hoaxbusters - CIAC Hoax Pages - <http://hoaxbuster.ciac.org/>
- 2) Purportal - <http://www.purportal.com/>
- 3) Stiller Research - <http://www.stiller.com/stiller.htm>
- 4) Urban Legends Reference Pages - <http://www.snopes.com/index.asp>
- 5) Urban Legends and Folklore - <http://urbanlegends.about.com/>

Are These Hoaxes? Now You Know How to Distinguish Fact From Fiction:

- 1) Are Sabrina Fair Allen and Penny Brown really missing children?
- 2) Are Bugbear and JDBGMGR.EXE (the Bear Virus) real viruses?
- 3) Should you sign a petition to keep a Nigerian woman from being stoned to death?
- 4) Are Christians being urged to boycott Dr. Pepper because the company omitted "Under God" from cans that had the Pledge of Allegiance on it?

Copyright 2002 by Daily Journal. Reprinted with permission.