



FEDERATION OF AMERICAN CONSUMERS AND TRAVELERS - NEWS RELEASE -

FOR IMMEDIATE RELEASE

Identifying Hoaxes and Urban Legends

EDWARDSVILLE, IL, September 7, 2009 - The National Cyber Alert System (a service from the Department of Homeland Security) has put together some tips and links that could help you safeguard yourself and your personal/business technology against fraud and attack. Here are some basic facts, especially in relation to the well-known “chain letter”:

Why are chain letters a problem?

The most serious problem is from chain letters that mask viruses or other malicious activity. But even the ones that seem harmless may have negative repercussions if you forward them:

1. They consume bandwidth or space within the recipient's inbox
2. They force people you know to waste time sifting through the messages and possibly taking time to verify the information, and
3. They spread “hype” and, often, unnecessary fear and paranoia

There are two main types of chain letters:

Hoaxes. Hoaxes attempt to trick or defraud users. A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus. It could also be a scam that convinces users to send money or personal information. “Phishing” attacks could fall into this category.

Urban legends. Urban legends are designed to be redistributed and usually warn users of a threat or claim to be notifying them of important or urgent information. Another common form are the emails that promise users monetary rewards for forwarding the message or suggest that they are signing something that will be submitted to a particular group. Urban legends usually have no negative effect aside from wasted bandwidth and time.

How can you tell if the email is a hoax or urban legend?

Be especially cautious if the message has any of the characteristics listed below. These characteristics are just guidelines—not every hoax or urban legend has these attributes, and some legitimate messages may have some of these characteristics:

- It suggests tragic consequences for not performing some action
- It promises money or gift certificates for performing some action
- It offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- It claims it's not a hoax
- -There are multiple spelling or grammatical errors, or the logic is contradictory
- There is a statement urging you to forward the message
- It has already been forwarded multiple times (evident from the trail of email headers in the body of the message)

If you want to check the validity of an email, there are some Web sites that provide information about hoaxes and urban legends:

Urban Legends and Folklore - <http://urbanlegends.about.com/>

Urban Legends Reference Pages - <http://www.snopes.com/>

TruthOrFiction.com - <http://www.truthorfiction.com/>

Symantec Security Response Hoaxes - <http://www.symantec.com/avcenter/hoax.html>

McAfee Security Virus Hoaxes - <http://vil.mcafee.com/hoax.asp>

FACT was formed under the not-for-profit corporation laws of the District of Columbia in 1984, and currently serves more than 1 million consumers nationwide. Additional information on FACT may be found in the *Encyclopedia of Associations*, and by visiting the association's Web site (www.usafact.org). Informative, unbiased news bulletins are regularly disseminated by FACT to help its members remain current on matters which might seriously impact their lives. In addition to publishing consumer-related reports, the association provides more than 30 benefits for its members, ranging from [medical insurance](#) and [dental discounts](#) to [prescription drug savings](#) and [scholarships](#). FACT's administrative office is located at 318 Hillsboro Avenue, Edwardsville, IL 62025.