

Email ‘Chain Letters’ Identifying Hoaxes and Urban Legends

Do you know anyone who is waiting for a \$1000 check from Bill Gates or Microsoft, as a reward for ‘beta-testing’ email tracking software by forwarding an email to everyone in their address book?

Have you been solicited to provide a complete stranger (often from Nigeria)
“ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THESE TRAPPED FUNDS, US\$21,320,000.00 (TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS)”?

Ever received a warning like “*This information arrived this morning, from Microsoft and Norton. Please send it to everybody you know who accesses the Internet*” or been urged “WE NEED TO DO EVERYTHING POSSIBLE TO STOP THIS VIRUS”?

Email messages with contents such as these are familiar to nearly everyone who has an email account. Some are sent by strangers, others by (usually) well-intentioned friends or family members. Regardless of content or source, email ‘chain letters’ are potential problems. These problems range from being a potential annoyance, through being the vector for malicious virus or worm attacks, to resulting in significant damage due to fraud or criminal activity.

When you receive a chain-letter message, and ‘pass it on’, you should be aware of and consider the implications of doing so. Even the most harmless, funny, cute, or inspirational chain messages:

- use network/Internet bandwidth during transport.
- consume storage space on mail servers and inboxes (picture and music files in particular can be very large).
- require the recipient to take the time to open and at least screen the content for value.
- may offend and/or annoy some recipients

This doesn’t mean you shouldn’t share these type messages to people you know would enjoy/benefit from them, but you should definitely consider to whom (and to where)

you are sending the messages; it is highly unlikely everyone in your address book needs or wants to receive them.

Some messages should not be forwarded—hoaxes and ‘urban legends.’

Hoaxes and ‘urban legends’ both attempt to trick or defraud users. The three previous examples are examples of common ones. A hoax message is often intentionally malicious, such as instructing the recipient to delete a file necessary to the operating system by claiming it is a virus.

Intentionally malicious hoaxes also include scams attempting to convince recipients to send money or personal information—[*phishing*](#) messages are malicious hoaxes.

‘Urban legends’ are hoaxes that are not overtly malicious but try to convince the recipient of an unlikely event or to take some unnecessary action, nearly always instructing the recipient to ‘send to as many others as possible’. Common topics of urban legends include dire warnings about new and devastating viruses (and the A-V vendors don’t know about them!), free money offers, reports of children in trouble, and requests for boycott of a product or company due to a rumored policy or action. Urban legends generally have few tangible negative effects (other than the resource issues above), but do result in significant

lost time as people sift through and attempt to verify information, and they result in the spreading of hype, fear, and paranoia.

How can you recognize a hoax or urban legend message?

Some messages are more suspicious than others, but ‘warning flags’ should activate if a message has many of these characteristics:

- there is a statement urging you to forward the message.
- it has already been forwarded multiple times (evident from the trail of email headers or multiple <FW>).
- it claims it's not a hoax.
- it suggests tragic consequences for not performing some action (including sending it on!).
- it promises money, gift certificates, or other reward for performing some action (especially passing it on!).
- there are multiple spelling or grammatical errors, or the logic is suspect or contradictory.
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software (NEVER follow the instructions or open the attachment...you will likely be infecting yourself!).

It looks like it might be legitimate...how do I know if it's not?

If you want to check the validity of an email, there are many web sites that provide information about hoaxes and urban legends. Some of the most popular are:

- Urban Legends and Folklore - <http://urbanlegends.about.com/>
- Urban Legends Reference Pages - <http://www.snopes.com/>
- Hoaxbusters - <http://hoaxbusters.ciac.org/>
- TruthOrFiction.com - <http://www.truthorfiction.com/>

What should I do when I receive a hoax or urban legend message?

The most important thing you can do is actually a ‘not do’—**do not** forward the message or follow its instructions!

If the message is a confirmed urban legend or other non-malicious hoax, simply **delete** the message. If you know the message sender well (particularly if the sender is an email or Internet novice), you may wish to help teach them about email chain letters—*individually and privately* (feel free to send them this article if you think it will help). In most cases, sending a follow-up ‘this is a hoax’ message to all original recipients is not effective or desirable.

If the message is a ‘warning’ about a virus or other malicious code, validate it via a reliable source before taking any action. If you can’t validate the information, it is very likely a hoax—information security organizations and vendors rapidly publish information on known exploits. Reliable sources include your organization’s information security office, anti-virus vendors’ web sites, information security specific sites such as CERT, CIAC, or SANS. Links to some reliable sites are:

- A-V Vendor Symantec (Norton)- <http://www.symantec.com/>
- A-V Vendor McAfee - <http://www.mcafee.com/>
- A-V Vendor Sophos – <http://www.sophos.com>
- Microsoft- <http://www.microsoft.com/security>
- CIAC- <http://www.ciac.org>
- CERT- <http://www.cert.org>
- SANS- <http://www.sans.org>

Dan O’Callaghan
Chief Information Security Officer
Sinclair Community College