



Enterprise Security Office Monthly Security Tips

NEWSLETTER

AUGUST 2007

Volume 2, Issue 8

Internet Hoaxes and Urban Legends

We have all received emails promising get-rich-quick schemes, warning of major computer meltdowns or images exploiting the latest natural disaster. These emails are more than just an annoyance; they do have a purpose, which is often malicious. Besides bogging down networks and clogging inboxes, they are also used by spammers to harvest email addresses, spread viruses, attempt to defraud the recipient, or unnecessarily cause fear and paranoia.

Often the messages they contain are untrue but a few of the sympathy messages in past hoaxes have been based on real events. Some hoaxes or malicious emails also use sensational news items like earthquakes, plane crashes, or terrorism incidents to entice people to open attachments and forward the message to others. Email messages written with the intention of the recipient sending it to people they know are known as chain letters. Hoax messages use several different methods of social engineering such as shock, curiosity, fear, and sympathy to get you to pass them along.

Chain letters may be sent by strangers or well-intentioned friends or family members. It is important to verify the information before following any instructions or passing the message along.

What are some types of chain letters?

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 have no negative effect aside from wasted bandwidth and time.

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

Some messages are more suspicious than others, but 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).

What are some of the latest hoaxes and legends circulating today?

- **Nigerian Scam** – A wealthy foreigner who needs help moving millions of dollars from his homeland promises a hefty percentage of this fortune as a reward for assisting him. Status: *Real fraud that costs its victim anywhere from a few thousand dollars to up to hundreds of thousands.*
- **Thousand Dollar Bill** – You can receive rewards from various companies by simply forwarding an e-mail message to your friends. This includes cash rewards to Internet users for forwarding messages to test a Microsoft/AOL e-mail tracking system. Status: *False.*
- **Cell Phone Directory and Telemarketers** – Email claims users must sign up with the national Do Not Call list to prevent telemarketers from calling their cell phones. Status: *False.*

- **Postcard** – A wave of malicious messages sent out with subject lines such as “You’ve received a postcard from a family member!” Status: *Real*. The e-mail attempts to induce recipients into clicking links that install a variant of the Storm Trojan.
- **Jury Duty Scam** – Identity thieves trick the unwary into revealing their personal details by telling them they’ve failed to report for jury duty and warrants for their arrest are being issued. Status: *Real fraud, potential for financial harm unknown*.
- **Help My Baby Live** – You should donate money to help an expectant couple seeking to raise \$50,000 in order to avoid opting for an abortion. Status: *False*.

What can I do to protect myself and my organization?

- If you get an email warning about a virus, call your help desk, or if you experience this at home, run your own anti-virus.
- Do not circulate warnings or suspect messages without first checking with an authoritative source. For example, check the hoax sites listed below.
- Don’t forward chain letters.
- Never open an email attachment unless you know what it is, even if it’s from someone you know and trust.
- Keep your anti-virus software up to date.
- Remember, cyber security is everyone’s responsibility.

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/>
- Hoaxbusters – <http://hoaxbusters.ciac.org>
- 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>



<http://www.msisac.org>