WV Executive Branch Privacy Tip

As you know, the Privacy Office occasionally issues tips to assist you in making informed decisions in your "away from work" life. The following tip is for that purpose and is from US-CERT (United States Computer Emergency Readiness Team), a part of the Department of Homeland Security.

Security Tip (ST04-009) Identifying Hoaxes and Urban Legends

Chain letters are familiar to anyone with an email account, whether they are sent by strangers or well-intentioned friends or family members. Try to verify the information before following any instructions or passing the message along.

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:

- they consume bandwidth or space within the recipient's inbox
- you force people you know to waste time sifting through the messages and possibly taking time to verify the information
- you are spreading hype and, often, unnecessary fear and paranoia

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 (see Avoiding Social Engineering and Phishing Attacks for more information).
- **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?

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)

  If you want to check the validity of an email, there are some websites that provide information about hoaxes and urban legends:
- Urban Legends and Folklore - http://urbanlegends.about.com
- Urban Legends Reference Pages - http://m.snopes.com/whats-new/
- TruthOrFiction.com - http://www.truthorfiction.com
- Symantec Security Response Hoaxes - http://www.symantec.com/avcenter/hoax.html
- McAfee Security Virus Hoaxes - http://home.mcafee.com/VirusInfo/VirusHoaxes.aspx

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.