DON'T BE AN APRIL FOOL: DON'T SPREAD HOAXES AND FAKE NEWS

We all know someone who has to be the first to share the latest viral video, “safety” warning, or urban legend. Naively passing on hoaxes leads to clogged mailboxes, and creates expensive bandwidth problems.

URBAN LEGENDS AND VIRAL MEMES

What is an Urban Legend?

Internet Hoaxes have one goal: multiply! If you send one to all your contacts, you unwittingly bog down Internet traffic. An urban legend may be a story you hear by word of mouth from an acquaintance or family member, or a message you receive via forwarded email, text, or social media. All urban legends have certain features in common. Contrary to popular belief, they aren’t always false. One identifying factor is that it’s told as if it were true regardless of the facts (the solemn word of “a friend of a friend of my sister” doesn’t make it factual).

Online versions of urban legends tend to be rewritten in the form of warnings or alerts and lose some of their story-like qualities. They also tend to become fixed, boilerplate texts, less susceptible to change, but they’re still urban legends.

Reposting urban legends and viral memes is not without risk. By the time a single viral image makes the rounds from its originating source to another social channel, blogs, and eventually BuzzFeed; the joke is over or the damage is done. Each image created by the world’s meme makers is open to constant speculation, revision, and endless re-postings.

If you don’t know who the person in the image is, or the story behind it, and you can’t verify it’s true — post or tweet about something else instead. We’ve seen well-meaning individuals, even law enforcement officials, take a "dire warning"-type meme, treat it as truth, and repost it. Perpetuation by a “trusted authority” of something that is not real, nor dangerous, undermines credibility and can contribute to disbelief when those authorities post about a real threat.

For more information on Urban Legends visit Digiknow.

FAKE NEWS AND HOAXES

What’s the Fuss about “Fake” News?

Leaving politics aside, our digitally-driven world is an information explosion every moment of every day. Cyber criminals and other disruptive types take advantage of human impulsivity to rush to post first.

Trending topics drive news cycles because, when thousands of people engage in an activity or use a term or hashtag, it becomes “news.” The human impulse to jump on the latest digital bandwagon contributes the spread of both “fake” news and hoaxes online. Hoaxes attempt to trick or defraud users while “fake” news damages trust in individuals and institutions.

Questions to ask before you repost or share:

Who Published It? Obscure websites plastered with ads and all-caps headlines should arouse skepticism. Googling a site’s name and checking out other articles it posts may shed light on whether it’s trustworthy. The Media Bias Chart may even help determine where a news source falls on a spectrum of factual reporting versus opinion.

What’s the byline date/time? Another common element in fake news is that old articles or events can resurface and lead people to believe they just happened. Checking the publishing time stamp is something you can quickly do to prevent being misled.

Are links/sources noted? A lack of links or sources for claims in an article is an obvious warning sign that the post is likely false.

Are multiple sources reporting on it? If a story looks suspicious or claims to reveal major news, search to see if other news outlets are also reporting the story.

Think Before You Share. Fake news sites prey on emotions and rely on the reader’s impulsive reaction to spread these stories without verifying them first. In extreme cases, these fake articles can balloon out of control and have serious consequences.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, want to print a PDF copy or view previous Newsletters, go to:

https://digiknow.dti.delaware.gov/pages/cybersecuritynewsletters.shtml