Position Paper

In this age of rapid communication by Internet, the prevalence of "spin" in the mass media, and the ease with which people can forward email messages that are false, misleading, or otherwise objectionable, we need to be alert to misinformation and find ways to deal with it. Urban legends about alleged deeds or statements made by public figures have increasingly become false, exaggerated, or even vitriolic. Voters are being given wrong or incomplete information about public policy so that they act with emotion rather than reason. Because we are often in a position of advocacy for human rights, the Social Action Committee is compiling a list of resources for checking facts and making sure we get the stories straight. The information we have collected is just a tool to be used as members wish, and we will continue to add resources to our list. Since our members have varying degrees of computer literacy, we define terms as if for beginners.

Guide to coping with junk email, chain mail, hoaxes, spamming, scams, and phishing.

Junk email is closely analogous to the junk mail that we all get in the US mail. Basically it is any email that is sent out without regard to whether the recipient is actually interested in it. It may be advertising goods or services, it may be expounding an ideology, it may be anything else that you don't want to receive. It is easy and cheap to send email; therefore can be used by a wide range of senders, some of whom may be of questionable character. It can be sent completely indiscriminately.

Spam: Sending the same mail to large numbers of people is known as "**spamming".**

If you receive such mail, you have not necessarily been specially targeted. There are many companies (mostly in the US) which sell lists of email addresses, which they gather indiscriminately from any source they can find, such as mailing lists, newsgroups, requests for information from on-line sources, etc. Your **internet service provider, or ISP,** will probably have a **"spam filter"** that flags suspicious email messages. You can report a spam message to your ISP so they will block the sender for future emails (look for a click-button labeled "spam" somewhere around your email "mailbox").

Chain email asks you to send a particular message to a number of other people, who are also asked to send it on. These messages can ostensibly for "good luck", to advertise a "worthy cause" or "religious inspiration" schemes. **Beware of those** that have been forwarded a number of times (usually indicated by vertical lines on the left margin), because they may contain "viruses" or "malware" intended to do harm or gather sensitive information from your computer. To stop well-meaning friends or relatives from sending you unwanted chain mail, you can ask them politely not to forward such messages. But if you think the email is trying to spread a deceptive message, such as a campaign falsehood, use a fact-checker such as www.FactCheck.org or www.FlackCheck.org and send a "reply to all" with the corrected information.

Hoaxes and Urban Legends are untrue stories designed to alarm or astonish gullible folks who pass them along as fact. Some of these legends have circulated for years, despite their having been refuted. When a message is forwarded rapidly to a wide audience, it is said to have "**gone viral**." One respected source for identifying rumors and urban legends is www.Snopes.com .

One popular type of chain email comes in the form of **hoax virus warnings**. The message usually purports to alert you to the existence of some new virus and urges you to pass on the message to everyone you know. **Do not** pass on such virus warnings.

Phishing: One sophisticated kind of scam is called **Phishing (sounds like "fishing").** The message asks you to follow a link to another web site where you will be asked for personal or sensitive information such as a password or your social security number. The sender often pretends to be a legitimate business or organization, and some may even mimic a web site that looks like the official one. Legitimate businesses would not email you to ask for such information. Instead of clicking on the phony link, type the company's web site into your browser and report the suspicious activity to their customer service department. It's wise never to give out your credit card numbers over the Internet or your telephone unless YOU have initiated the contact.

A **podcast** is an Internet radio show, named by combining the word "broadcast" with the Apple iPod. **Podcasts** are usually free to listen to and range over a variety of topics. You can sign up for these free podcasts using free podcast software available online. Sometimes you will want to fact-check a statement made in a podcast.

Somewhat like a podcast is a **Twitter account. Twitter** is a service for friends, family, co–workers and other groups to communicate and stay connected through the exchange of quick, frequent questions and answers. They are often sent by cellphones or "smart phones" as well as computers. The messages, called **"Tweets,"** are limited to 140 characters. Because a Twitter network can contain large numbers of addresses (called "handles," beginning with an @ sign), a single Tweet can reach thousands, and any of them can "retweet" (RT) to forward the brief message to other individuals or groups. If you are trying to reach a large audience through a Twitter account, you can keep track of retweets to get an idea of the extent to which members of your network share ideas. Some retweets are messages you have previously tweeted that followers of yours have retweeted to their own networks. Other retweets are tweets of people you follow who posted that you've retweeted to your network. Only retweeted tweets that contain your Twitter username show up in your list of retweets.
Tutorials showing you how to use Twitter are available at the web site www.Twitter.com

---

Special warning about hotlinks ending .exe

A "hotlink" is a web address or email address underlined in blue that takes you to another site when you "click" on it. The extension .exe on a hotlink means "executable" which will create a file on your computer with a hidden set of directions for the file to execute, or carry out. Do NOT click on any hotlink sent to you by email. It may do damage to your computer or put in place some malware or spying instructions. Do NOT forward such suspicious links to other people.

Facebook Hacking & Safety

Your Facebook account is a virtual portal to information, media and an online social presence. Here, too, people can post messages or pictures and forward received messages to other friends (in fact, "to friend" is now a verb). You can click on a button with a thumbs-up icon if you approve comments made on Facebook pages or on a "like" button). Forwarded messages or pictures are supposed to follow rules of courtesy, but some offensive messages may get through. You can usually report an objectionable comment to the administrators of the program by clicking on a link near the comment.

Merely having a Facebook account puts you at risk of having your profile commandeered by spammers or used for Facebook scams. By knowing how you put yourself at risk, you can better protect your account and subsequently all of your Facebook friends. Although spammers and scammers can try to hack into your account, with proper protections and practices you're less likely to be affected.

For more information: Facebook Hacking & Safety | eHow.com
http://www.ehow.com/info_8701127_facebook-hacking-safety.html#ixzz2EK70Y6Nr

Resources for checking on validity

FACTCHECK.ORG
A PROJECT OF THE ANNENBERG PUBLIC POLICY CENTER

FactCheck.org launched in 2007. Lori Robertson posted some tips on March 18, 2008:

"I've noticed that chain e-mails, particularly those about politics, have a lot of things in common: urgent and frightening messages; spelling errors; a tendency to blame mainstream media for not telling the real story; and false, misleading, utterly bogus, and completely off-base claims.

We at FactCheck.org ask the public to be skeptical about politicians' claims. With these e-mails, outright cynicism is justified. Assume all such messages are wrong, and you'll be right most of the time. Yes, there are a few chain e-mails floating around the Web that are actually true – but not many. And when it comes to messages about the top presidential contenders, truth in e-mail is an elusive quality. While a handful had elements of truth in them or couldn't be verified, the vast majority were flat-out false."

Snopes.com, founded by Barbara and David Mikkelson, has been investigating e-mail and other urban legends since 1995. They list the investigated info in categories, such as religion and politics. Under the category of Urban Legends is this one about scientists allegedly finding the Lost Day of Joshua in the Bible. http://www.snopes.com/religion/lostday.asp#TQD2jYRBXR3iTjuI.99

About.com Another writer who debunks rumor and lore is David Emery, author of **About.com's Urban Legends** page. Investigating seven e-mails about Hillary Clinton and five about Barack Obama, he found all 12 false and misleading. Emery says in 10 years of this line of work, he has looked into a thousand or so e-mails. Most of them contain a mixture of facts and falsehoods.

How To Spot an Email or Chain Mail Hoax

This advice is adapted from internet postings on **About.com**, by David Emery, and the **FactCheck.org** site, by Lori Robertson.

Here's a list of common signs to watch for:

- Virtually any email chain letter you receive (i.e., any message forwarded multiple times before it got to you) is more likely to be false than true. You should automatically be skeptical of chain letters. Those with sloppy writing and misspelled words are probably not authentic.

- Note whether the text you've received was actually written by the person who sent it. Did anyone sign their name to it? If not, be skeptical. Also, be aware that friends' names might have been "hijacked"; so check with them to see if they really sent it. They may need to change their email addresses.

- Look for the telltale phrase, 'Forward this to everyone you know!' The more urgent the plea sounds, the more suspect the message. It's especially dubious if the message is anonymous or tells you not to forward it if you don't agree.

- Look for statements like 'This is NOT a hoax' or 'This is NOT an urban legend.' The more insistent the senders are, the more likely that it IS a hoax.

- Watch for overly emphatic language, as well as frequent use of UPPERCASE LETTERS and multiple exclamation points!!!!!!!

- If the text seems aimed more at persuading you or selling something than informing you, be suspicious. Like propagandists, hoaxers are more interested in pushing people's emotional buttons than communicating accurate information.

- If the message purports to give you extremely important information that you've never heard of before or read elsewhere in legitimate venues, be very suspicious. Hoaxers usually try every means possible to make their lies believable -- e.g., mimicking a journalistic style, attributing the text to a 'legitimate' source, or implying that powerful corporate or government interests have tried to keep the information from you.

- Read carefully and think critically about what the message says, looking for logical inconsistencies, violations of common sense and blatantly false or exaggerated claims.

- Be especially wary of health-related rumors. Most importantly, never act on 'medical information' forwarded from unknown sources without first verifying its accuracy with a doctor or other reliable source.

- Check for references to outside sources of information. Hoaxes don't typically cite verifiable evidence, nor link to Websites with corroborating information. Also, verify that the linked reference actually supports the position of the messenger; some references say the exact opposite of what they have been alleged to support.

- Check to see if the message has been debunked by Websites that debunk urban legends and Internet hoaxes (such as Snopes.com, FactCheck.org, or FlackCheck.org).

- Research any factual claims in the text to see if there is published evidence to support them. If you find none, odds are you've been the recipient of an email hoax.

- If a famous person is cited as an authority on the issue in the email message, check to see whether that person is actually listed in Who's Who or among the faculty-staff of the institution where he or she allegedly works.

- If there is math involved in the claims of an e-mail, do the math! It is probably wrong.

Then, there's a little thing called "spin." You can take a string of incontrovertible facts and present them in such a way that they point to a false conclusion. To combat this tendency in email and mass media, **FlackCheck.org**, a sister organization to **FactCheck.org** was established at the Annenberg Public Policy Center of the University of Pennsylvania.

FLACKCHECK.ORG A Guide for Political Literacy and Engagement

FlackCheck.org is a video-based counterpart to APPC's award-winning program FactCheck.org. FlackCheck.org uses parody and humor to debunk false political advertising, poke fun at extreme language, and hold the media accountable for their reporting on political campaigns.

FlackCheck.org is funded by an endowment provided by the Annenberg Foundation to support the Leonore Annenberg Institute for Civics and by a grant from the Omidyar Network.

Here is a sample of a question sent to FlackCheck.org (Link leads to a more complete answer).

Is the ACLU suing to have cross-shaped headstones removed from military cemeteries?

The ACLU has filed no such suit, and it hasn't sued to "end prayer from the military" either.

July 5, 2009

The complete answer by FlackCheck explains the mistakes in this rumor (the ACLU actually was favorable to the headstone symbols as long as non-Christians were also welcome to use their own icons). FlackCheck also rebuts the false rumor that prayer is not permitted in the military, and the misperception that arose when a chaplain who was disciplined for violating a dress code claimed he had been discriminated against for using the name "Jesus" in a sermon. The ACLU had nothing to do with that case.