**Overview 1, Government Distrust Focused:**

**People lose out on valuable services when there is a broad distrust of government.**In particular, makes it difficult for real government agencies to contact citizens and provide the services that their taxes pay for. Below are a set of tips on how to recognize real communications from government agencies. **Please review them carefully.**

**Overview 2, Internet Distrust Focused:**

**People lose out when they generally distrust the Internet.**In particular, that distrust makes it difficult for them to benefit from the ready-to-find information, online shopping, and even e-government services. Below are a set of tips on how to recognize real communications from companies and government agencies. **Please review them carefully.**

**Overview 3, Scammer Focused:**

**Have you ever wondered if a website or email message is real?**

Scammers sometimes pose as government agencies or well-known companies, in order to trick their victims into providing personal information about themselves. In additional to stealing information (and money), this has led some people to distrust the Internet generally – and miss out on its benefits.  
  
**You can learn to tell the difference**between real websites and emails and fake ones, so you don’t get tricked, and you don’t miss out. Below are a set of tips on how to recognize the real, trustworthy ones. **Please review them carefully.**

**Tips**

1. Before you click on a link, look at where it’s trying to take you. Is it from a .gov or well known .com address? .Gov domains are very difficult to fake; so are well-known addresses like “Amazon.com”.
2. After you click, double check where it’s located. Look at address at the top of the browser. Is it actually a .Gov or well-known address?
3. For emails, look at the “mailed by” field in the headers. That must also be from a well-known address or .Gov domains; official looking communications that are gmail, yahoo or similar sites are a giveaway.
4. While misspelled words are often a giveaway of a scammer, a professional-looking site or email doesn’t mean it’s trustworthy.
5. Anytime a company or government agency that you didn’t directly contact reaches out to you and requests your personal information.
6. Similarly, anytime a company or government agency that you didn’t directly contact reaches out to you to ask for or even offer money.  Scammers can use the offer of money to get your bank account information and rob you.

In addition, please follow standard safely measures online: make sure you only enter information on secure (‘HTTPS’) websites. Make sure also you have virus protection and a firewall in place, and it’s up to date. These won’t help you specifically against scammers, but they can help you against other online attacks.