AADMM
American Association of Daily Money Managers

Email/Phishing Scams

The following are tips to avoid email/phishing schemes:

- The IRS **DOES NOT** send out emails! If you receive an email allegedly from the IRS, delete it immediately! This is not a legitimate email. **The IRS will never contact you via email.**
- Be cautious of any emails sent with no subject or the subject is "Hi." These types of emails are usually designed to catch the user off-guard, and typically asks you to click on a link or perform a similar action.
- Be aware of legitimate-looking company emails, usually involving a purchase. Emails referring to a FedEx delivery or Amazon order should be confirmed **before** you respond to an email. Make sure you know exactly how a company will contact you if you have made a purchase/placed an order.
- Take a look at the sender's email address. Often, scam emails are sent allegedly from someone you know. They may have the correct name and the message may even seem legitimate, but once you look at the sender's email address, it appears to be fake. For example, you receive an email from your friend Bob who works at the Maryland U.S. Department of Transportation. Bob's regular email address is bobsmith@dot.md.us.gov, however, the email address of the sender shows bobsmith@576rt&^%$.us.gov, this is likely a fake email. If a sender's email address appears odd or suspicious, it probably is. Delete it immediately, do not click on any links within.
- Never give any information to someone posing on-line as an organization that wants your assistance. Always verify the credentials of an organization before responding via email.
- If you get an email with information that sounds too good to be true, it probably is. For example, you receive an email from someone claiming to be an African prince who promises to share 25% of his $5 million-dollar inheritance with you if you if you assist him in some way. (Too good to be true? You bet!) Delete it immediately.
- Do not engage with a person sending an unsolicited or unexpected email, even if you think it may be legitimate. Often, these emails are designed to get you comfortable with the sender so they can obtain information from you. Sometimes they already have some of your information and are looking for you to complete the missing components.
- Never, never, never click on any links that accompany an email, especially if you have some doubt about the veracity of the email.

Here are some additional tips and resources to prevent fraud and identity theft

THE AMERICAN ASSOCIATION OF DAILY MONEY MANAGERS (AADMM)

AADMM is a national membership organization representing individuals and businesses in the growing profession of daily money management. These professionals provide financial services to seniors and older adults, people with disabilities, busy professionals, high net worth individuals, small businesses and others. AADMM's mission is to support daily money management services in an ethical manner, to provide information and education to members and the public, and to develop a network of dedicated professionals.

For more information, contact:
American Association of Daily Money Managers
174 Crestview Drive, Bellefonte, PA 16823-8516
Phone: 814-357-9191 | Email: info@aadmm.com