Email Scams

According to the MetLife Study of Elder Financial Abuse, older Americans lose approximately $2.6 billion to fraud each year. Common email scams that use fraud include grandparent scams, sweepstakes scams, phony charities, free meal solicitations, fake debt collectors, and health care scams, according to the Cuyahoga County Department of Consumer Affairs:

- **Grandparent scams** consist of the third party sender posing as a grandchild requesting money through a wire transfer during an emergency. This tactics may be thwarted by not wiring money before calling the family member to verify the situation.
- **Sweepstakes scams** consist of an email claiming that the recipient has won a prize, and must click a link to claim it. This link most likely will contain computer programs, such as malware or ransomware, which will steal the user's information that can subject the victim to identity theft. This method may be checked by not opening suspicious emails or clicking suspicious links.
- **Phony charities** consist of a third parties posing as a charity to collect funds for their personal use. The best method to check this tactic is to confirm the party is registered as an official reputable charity.
- **Free meal solicitations** consist of third parties offering the proverbial free lunch; however, there could be strings attached. The best way to avoid this kind of scam is to investigate the company offering the free meal solicitation.
- **Fake debt collectors** seek to scare the caller into revealing nonpublic financial information, such as bank account numbers, routing numbers, credit card information, or debt card information, by threatening arrest, shutting off account access, or foreclosure. This scheme may be checked by looking up the company's name and information. Do not provide any financial information until you confirm that the company is legitimate.
- **Health care scams** consist of third parties posing as Medicaid, Medicare, Social Security officials or as representatives of medical services. Do not give away your information unless you can verify the third parties are the persons they claim to be, such as the email arriving from an official government email.

General tips for avoiding email scams include not clicking on suspicious emails or link. An email may appear to be suspicious if it contains numerous misspellings, comes from an email account you do not recognize, or has a topic the individual would be unlikely to email about, such as a grandchild talking about investing in a new home if the child is an adolescent. A link may be suspicious if it seems out of place or if you do not recognize the website.

In the event of encountering an email scam, please report it to the Cuyahoga County Department of Consumer Affairs, which may be reached at http://consumeraffairs.cuyahoga county.us/en-US/home.aspx or 216-443-7035, or the Ohio Attorney General's Office by visiting www.OhioProtects.org or calling 800-282-0515.