WINDSOR COA NEWS
April/May 2021

Our mission is to serve older Windsor adults by providing opportunities and resources that advance the quality of life in a rural community.

The Executive Office of Elder Affairs provides financial support for this COA publication.

If you are anything like me or the friends and neighbors with whom I have spoken, you are receiving an increasing number of annoying and persistent calls and emails, many of which can be classified as "scams." My most recent one was a recorded call from "Amazon" telling me that an Apple IPhone had been ordered and billed to my account. I needed to "press 1" to cancel the order. ***I hung up!*** Then I called the real Amazon and spoke to a lovely woman in customer service who assured me that my account had not been compromised. She followed up our phone conversation with an email with some very good information.

The call I received was a "phishing scam." I went looking for more information and found copious amounts of advice, not only from Amazon, but also local banks and the Better Business Bureau (www.bbb.org) among others. I encourage you to research and learn more as I did.

Here are ten tips to avoid scams from the Better Business Bureau.

1. **Never send money via gift card or wire transfer to someone you have never met face-to-face.** These cannot be traced and are as good as cash, and chances are, you won't see your money again.
2. **Avoid clicking on links or opening attachment in unsolicited emails.** Links, if clicked, can download malware onto your computer, smart phone, tablet or whatever electronic device you're using at the time, allowing cyber thieves to steal your identity
3. **Don't believe everything you see.** Just because a website or email looks official does not mean that it is. Caller ID is commonly faked.
4. **Double check your online purchase is secure before checking out.** Look for the "https" in the URL (the extra s is for "secure") and a small lock icon on the address bar. Make certain you are on the site you intended to visit. (Many of us have been shopping more online this past year, and it is easy to click on a look alike site in a list, so double check). Read reviews and look for a physical address listing on the website itself and a working phone number. Take the extra step and call the number if it is a business you are not familiar with.
5. **Use extreme caution when dealing with anyone you've met online.** Scammers use dating websites, Craigslist, social medial and many other sites to reach potential targets.
6. **Never share personally identifiable information** with someone who has contact you unsolicited, whether it's over the phone, by email, on social media or even at your front door. This includes banking and credit card information, your birth date and Social Security/Social Insurance numbers.
7. **Resist pressure to act immediately.** Shady actors typically try to make you think something is scarce or a limited time offer, pushing victims to make a decision before

asking family members, friends or a financial advisor, and even advising you to "trust" them.

8. **Use secure and traceable transactions.** Do not pay by wire transfer, prepaid money card, gift card, or other non-traditional payment method. (See #1 above).Say NO to cash-only deals, high pressure sales tactics, high upfront payments and handshake deals without a contract. Read all of the small print on the contract and make sure to understand what the terms are.
9. **Whenever possible, work with local businesses.** Ask to see proper identification and proof of licensing and insurance, especially contractors coming into your home.
10. **Be cautious about what you share on social media.** Connect only with people you know. Check privacy settings on all social media and online accounts. Imposters often get information about their targets from their online interactions, and can make themselves sound like a friend or family member because they know so much about you. Then, update and change passwords to passphrases on a regular basis on all online accounts. [NOTE: Are you, too getting "friend requests" on face book from people you don't know and never heard of???]

It's also important to never give your personal information "to verify" your identity. If it doesn't seem right, hang up and call the company (bank, utility) at the number you know is right and not a number the caller gives you.

[Interesting fact from the BBB: The age group most likely to be scammed is 18-24!]

Survey Scam with a twist – Did you receive a text with a survey about your vaccine? The phony survey claims to be from pharmaceutical company Pfizer with questions about their COVID-19 vaccine. Here's how it works:

You receive an email or text message that claims to be Pfizer, one of the pharmaceutical companies producing an approved COVID-19 vaccine. In some versions the message claims that you will receive money for completing a quick survey. Other versions offer a "free" product. It sounds easy, but don't click on the link! These survey scams have a variety of tricks. The link may lead to a real survey, which upon completion, prompts you to sign up for a "free trial offer." Victims reported to the Better Business Scam Tracker that they entered their credit card information to pay what they thought was a shipping fee. Instead, the scammer billed them many times more and never sent the product. In other versions, the form is actually a phishing scam that requests banking and credit card information. Don't fall for it!

~~~~~~

REAL ID We have learned from AAA that there are many folks who are showing up at their offices wanting the REAL ID but don't have the proper information necessary. Also, appointments are needed at both the AAA and the RMV. Please plan ahead. AAA can be reached by calling 413-445-5635. It may take some time for them to answer as they are very short staffed. RMV needs to be contacted on line at mass.gov/ID. This is also the web site where you will find the REAL ID checklist for the documents you need to bring to your appointment. (If you do not have internet access and need a check list, call Sue at 684-3191).
~~~~~~