**Senior Scams**

The best way to spot a scam is by 3 things- 1. You do not know the caller/sender. 2. You have to pay a fee to get your money, prize, and 3. Say 'would you kindly' etc. Make sure to report any fraud by contacting your local Police Department. Many times scammers will ‘Spoof” which means the phone number they are really calling from is being copied with a known number.

* The first and most important lesson- if you do not know who it is DON’T answer it or open that email... Most scammers are very cunning and convincing.
* Secondly, you will never EVER use Western Union/Visa/Amex/Gift Cards/Apple/Google/Amazon/Steam/Xbox. You cannot pay rent/food/bail/fee/etc. with a gift card.

**Here are a few ways that people have been frauded out of hundreds of thousands of dollars**

* A relative says they are in jail and need you to bail them out. I have even had at least one that was so convinced her Grandson was in jail (She does not have any Grandkids) Very convincing!
* Scammer calls typically target the elders and people they can search easily online in the Public records. Make sure your cell phone is secured with a virus protection (Kaspersky is a great one).
* Emails and calls will tell you that if you do not take care of care of this speeding ticket or other minor infraction we are going to put you in jail- these are always scams.
* Payment for goods on Amazon, eBay, Google, Target, Walmart- if you have not seen, met with, or talked to in person the sale is probably a scam.
* Payment by Western Union- NEVER send money to someone you do not know. If it feels fishy, do noy hesitate to just block that caller and hang up!
* When necessary to pay for those above use a prepaid card such as Chime/Cash App/Venmo/PayPal instead of your debit card. Use a credit card for online purchases because you can dispute the charges.
* Don’t fall for giving out any personal info, including your name, address, social security number, credit card number. Have a burner card to use to pay for your online purchasers.
* Beware of dating sites, such as tinder, match, and chat rooms. There are always wats to scam you out of your life savings.
* The IRS will NEVER call you telling you that you need to pay anything. It’s a scam.
* Have secure passwords that are combination of numbers, letters, and special characters such as ?&\*$%. Use a password manager if needed. The most secure passwords are randomly generated. This goes with your security questions. When you use common ones like your first animal, make of your car, maiden name, spouses middle name, where you grew up. These are answers that are pretty east to find on the internet or you may have chatted with someone who you were telling them about your childhood, your favorite pet, your first car… Try another safer way to log in any app is to use 2 factor authenticator send you a text or call with code you have to put in before you can access your accounts

Here are great websites to see scams and stay informed

<https://www.usa.gov/scams-and-fraud>

<https://www.aarp.org/money/scams-fraud/?intcmp=AE-MON-CP-BB-LL>

<https://www.walgreens.com/topic/fraud_information.jsp>

 <https://www.consumeraffairs.com/scam_alerts/scam_alerts.htm>

 <https://fraud.org>

 <https://consumer.gov/section/scams-identity-theft>

* Finally, if you get a call don’t answer it but if you do, refrain from saying anything especially ‘yes’ or ‘no- they can use your voice to wipe you out of house and home

**Safety Tips**

* Be suspicious of unsolicited emails, phone calls, or text messages asking for personal or financial information.
* Never respond to emails or texts from someone you don't know or whose identity you can't confirm.
* Never provide personal or financial information unless you are certain of the identity of the person or business that is contacting you.
* Never open suspicious attachments or links.
* Never purchase something that was advertised in an unsolicited email.
* Never send money or other type of monetary payment to someone you don't know.
* If you are contacted by someone you don't know, conduct online research. You can search a phrase that describes the situation or look up the email or phone number that contacted you.
* If you're unsure if a phone call or email is really from the company it claims to be, call the number from their legitimate website. Do not call the number that initially called you or one provided in the email.
* Look closely at the sender's email address and embedded URL's. More sophisticated scammers will create fake domains and websites that look nearly identical to the legitimate business.
* Hover your mouse over a link to see the embedded URL. Do not click on the link if the address is different than the display text.
* Do not deposit a check that is sent to you with instructions to wire money back to the sender or a 3rd party. Banks are required by law to make deposited check funds available within days and identifying a fake check can take several weeks. If a check you deposit turns out to be fraudulent, you will be responsible for paying the bank back.
* Regularly monitor your financial statements to detect any fraudulent charges. If an unauthorized charge is made to your account, immediately contact your bank or account provider.