

Don't Fall Victim to **Financial Scams**

A financial scam can happen to anyone, scammers do not discriminate but they tend to target individuals aged 60 and over.

Scamming is a multi-billion dollar epidemic that is only growing. Being aware and alert is the best preventative tool.

If it sounds "Too Good to be True" - it's likely fraudulent

Scammers are professional liars and thieves - they have honed their craft and know EXACTLY how to prey on innocent victims. They use a variety of paths to get to their targets: Phone, Email, Direct Mail, the Internet and Social Media.

COMMON SCAMS

Medical Imposters including: posing as a Medicare/Insurance representative or selling counterfeit prescription drugs

Investment and Sweepstakes Schemes including: pyramid schemes, claims of winning a lotto or prize, and fake inheritances

Telemarketing/Phone Scams including: posing as utility companies, the IRS, or even charities

Internet Fraud including: phishing emails looking for personal information or to install viruses

Grandparent Schemes including: pretending to be the grandchild and asking for money or pretending to have kidnapped a grandchild - both request either a Western Union payment or gift cards

Online Dating Scams where your date requests money to support them

Facebook Ads where fraudulent companies sell you something and never deliver

For tips on how to protect yourself and loved ones

Financial Fraud Prevention

Be ALERT, AWARE and ASK QUESTIONS!

If it Sounds too Good to be True it's Probably a Scam. There are no legitimate lotteries or sweepstakes that would require you to send them money in order to collect ANYTHING in return.

Don't Hesitate to Ask a Friend or Family Member. No legitimate business will make you agree to anything on the spot. If you are unsure, run it by someone else.

Don't Answer Calls or Emails from Unfamiliar Sources. Go directly to the company's website or call using their public phone number. Do a Google search and look for reviews from other people. Anyone can have a website - that doesn't mean they are a legitimate or honorable husiness!

Be Wary of Western Union or Gift Card Requests: If someone calls looking for these types of payments, they don't want a paper trail. 99.9% of the time this is a scam.

Don't be Click Happy. Email is one of the easiest ways scammers collect your personal information. NEVER download a file or click on a link from someone you do not know. Doing so will often result in malware or a virus infecting your computer allowing the scammer to get all the data they need.

NEVER Send Personal Information via Unsecured Email. No legitimate bank or company will ever ask you to send personal information (date of birth, social security number, credit care/banking information) via email unless it's sent via secure email which would require a log in.

Don't be Lured by "FREE" and "HUGE DISCOUNTS" When it Comes to Prescription Drugs. Often these drugs are NOT legitimate deeming them unsafe. Stick with reliable pharmacies suggested by your doctor or insurance carrier.

Report It: If you feel like you have been financially exploited immediately call your bank or credit card company AND the police. The sooner your accounts are flagged the better.

CONNECTICUT MUTUAL HOLDING COMPANY







www.collinsvillebank.com 860.693.6936



www.nwcommunitybank.com (860) 379-7561



Member FDIC

