12/12/23

Good morning CSH and Happy Holidays

I hope everyone and your families are healthy.

The Holiday Season is a busy season spent with friends and family. Unfortunately, it is also a time when scammers look to take advantage of our busyness and good nature. The U.S. Attorney's Office has put together a listing of common holiday scams. Below is synopsis of the listing, this link is the full posting.

Fake Online Stores or "Lookalike Stores." Be on the lookout for online stores that are either entirely fake or made to look like a legitimate store.

Missed Delivery/Non-Delivery Notification. With the rise in online shopping, lots of packages arrive at our front door during the holiday season. Beware of fake delivery notification emails or text messages alerting you of a missed package delivery.

Gift Card Scams. Gift card scams involve either scamming consumers into buying fake gift cards or tricking consumers into using gift cards to pay for fraudulent goods or services.

Fake Charities. During the holidays, cybercriminals seek to take advantage of consumers' generosity through fraudulent charities, GoFundMe campaigns, and other charitable causes.

Phishing Emails or Texts. Cybercriminals take advantage of the hustle and bustle of the holiday season to dupe consumers via phishing emails or texts that contain suspicious links. Be particularly mindful of purported communications from your bank or credit card company, warning you that your account has been compromised.

Fraudulent Seasonal Jobs. Employment scams tend to increase during the holiday season, as scammers prey on individuals seeking to make extra money. Be mindful of fake job ads, especially online job listings that offer good money for very little work.

Some examples of financial fraud targeting seniors are:

- **Lottery Phone Scams** – in which the callers convince seniors that a large fee or taxes must be paid before they can receive lottery winnings.
- **Grandparent Scams** – which convince seniors that their grandchildren are in trouble and need money to rent, repair a car, or even money for bail.

- **Romance Scams** – which lull victims to believe that their online paramour needs funds for a U.S. visit or some other purpose.
- **Tech Support Scams** – which convince victims to pay for non-existent problems with their computers.
- **IRS Imposter Scams** – which defraud victims by posing as IRS agents and claiming that victims owe back taxes.
- **Sham Business Opportunities** – which convince victims to invest in lucrative business opportunities or investments.

Below are some tips on how to avoid falling victim to a financial scam:

- Don't share personal information with anyone you don't know.
- Don't pay a fee for a prize or lottery winning.
- Don't click on pop-up ads or messages.
- Delete phishing emails and ignore harassing phone calls.
- Don't send gift cards, checks, money orders, wire money, or give your bank account information to a stranger.
- Don't fall for a high-pressure sales pitch or a lucrative business deal.
- If a scammer approaches you, take the time to talk to a friend or family member.
- Keep in mind that if you send money once, you'll be a target for life.
- Remember, it's not rude to say, "NO."
- A good rule of thumb is, if it's too good to be true, it's likely a scam.

Be well, my friends.

Please take care of yourself, and if you can take care of someone in need.