Be Aware: Financial Fraud and Scams

Criminals are always working to improve their methods of acquiring your personal information. While their techniques and strategies may evolve, there are some red flags you can watch for to safeguard yourself against threats.

- **Look for grammatical and spelling errors.** Legitimate organizations uphold high standards for their communication and do not have errors in their letters and documents.
- **Search online for information about the organization.** Verify contact information independently rather than relying on details provided in unsolicited messages. Scammers can change the name and number on caller ID, so never trust what the call states.
- **Exercise caution if an offer seems too good to be true.** Intuition often alerts us to potential scams, seek a second opinion if you are unsure. Doing so can help you see what red flags you may be missing.
- **SLOW DOWN!** Scammers often use urgency to intimidate you into quick decisions. They will tell you there is a time limit, and you HAVE to act now! They do this to get you in a panicked state and react before you slow down to think about what they're asking. Take your time and talk to someone else before you hand over any personal information or money, reputable organizations will have no problem with this.
- **Regularly monitor your financial accounts.** Utilize online banking and set alerts to notify you if there is unusual activity. If you notice anything odd on your accounts, contact your financial institution right away.
- **Do not pay upfront for "necessary expenses".** Be wary of scenarios that require you to make payments before you can access your "winnings", especially if you don't recall even signing up for the contest you've supposedly "won".
- **Think twice about free trial offers**. Some companies will offer you free shipping or a discount if you sign up for the free trial. Look at the terms and conditions to understand any automatic billing or hidden charges.
- **Never provide any personal information to an email inquiry.** The email may look like it is from Social Security Administration or even your financial institution, but reputable organizations do not solicit sensitive information via email. Contact the organization independently to verify if the email is legitimate.
- **Avoid clicking on links found inside emails.** These can by phishing links, could lead to a virus being installed on your computer, or even orchestrate a complete computer takeover demanding ransom money to regain access to your device.
- **Never deposit checks from an unknown source.** Check fraud is common and can take days to determine if the check is legitimate. Any money you spent from that check during that time could be lost in the scam.

In the event of a potential scam, seek guidance from trusted individuals or financial institutions immediately. Remember that you are not the first person that has fallen for a scam. By practicing caution and seeking assistance when in doubt, you can shield yourself from financial harm.