Customer Advisory: Use Caution Responding to Messaging Apps

Fraudsters are contacting potential victims on their phones to try to lure them into cryptocurrency scams with promises of guaranteed returns. Spot the fraud by remembering all trades involve a risk of loss. Be suspicious of any messages you receive via WhatsApp, Telegram, SnapChat, WeChat, SMS texts, or other apps that promise guaranteed oversized returns. If you receive a suspicious message:

- Do not reply.
- Delete the messages or group discussions and block the senders. Send text messages to junk.
- Review your privacy settings to protect your information and reduce future spam.

Deception in the Palm of Your Hand

By default, messaging apps allow anyone with your phone number to call or add you to a discussion group. Scammers use this vulnerability to add random or targeted phone numbers to WhatsApp groups or Telegram chats. You might see a message that you've been added to a group, then other messages follow. They might talk about trading crypto futures with leverage, "cooperative trading projects" (also called pump-and-dump schemes), 100, 500, 1,000 percent profits, advanced artificial intelligence, can't-miss investment *programs*, or other supposed opportunities. You might also see testimonials from other group members. It's all fake, lies designed to steal your money.

Don't Talk to Strangers

Stranger danger applies to your mobile device too. Responding or complaining confirms to scammers that your number is active and will only lead to more fraud attempts. The same is true for answering unknown callers. Scammers sometimes use robocalls to identify working numbers.

Caller ID can be easily faked. If you don't recognize the phone number, or message sender, do not respond. If you receive an urgent message about a financial account, or from law enforcement, the CFTC, or other government agencies, visit the entity's official website and confirm the message with customer service staff. Do not use phone numbers or links provided in the message.

You should only trade futures with regulated individuals and firms that follow strict qualification, supervision, and customer protection requirements. Learn more about registration at **cftc.gov/check**. Taking financial advice from unregistered, random people online or trading with unregistered companies that don't have a physical presence in the United States substantially increase your fraud risk.

Tighten your Security

Most apps let you adjust your privacy settings to only allow your contacts or specific numbers to message you or see your personal information, including your picture, location, and activity status. Check and adjust your settings in each app you use. Delete unwanted groups, block the admins, and report the groups and admins to the platform.

For SMS and phone messages, check your carrier's apps and account settings. Most major carriers offer free SMS spam and call blockers. Next, adjust phone and message settings on your device, including blocking unwanted callers or silencing spam calls. Activate options to filter unknown senders and junk. If you have the option to "delete and report junk," use it. If not, forward unwanted messages to 7726 (SPAM). Both options help filter and block bad actors systemwide.