The Office of Secretary of State
Securities and Charities Division

INVESTOR ALERT: Cryptocurrency Scam: Pig-Butchering
Issued: July 19, 2023

The Secretary of State's Division of Securities and Charities is issuing this Investor Alert to warn investors about the latest investment fraud, Pig-Butchering. This is a cryptocurrency scam that has been targeting Georgia investors this summer.

"Pig butchering scams" as they were named in southeast Asia, are scams where scammers build the victim's confidence through casual conversation with a real person who eventually convinces the victim that they will help them make money. It's called "pig butchering" because the alleged scammer continually feeds the victim information as they fatten the victim with excitement and the promise of great investment returns.

Scam artists will use your phone number or address to contact you in an attempt to take your money if they can. Scammers also scour social media, business records and even dating sites to find information to target potential victims. They will contact you through social media, text messages, email, mail, Whatsapp etc.

HOW THE SCAM WORKS

The scammer may pretend to be an old friend, a trusted public figure, your boss or even a prospective romantic partner. The conversations will slowly begin to center around investments or cryptocurrency, asking questions about your financial background and investing habits. The scammer's goal is not to request money from you, but to convince you to invest in a fake trading website or platform that will show you a bogus balance with lots of profit.

The scammer will "fatten the pig" by allowing you to withdraw profits early so you will trust the process and invest more. They may even "lend" you money so that you can make larger trades. The promise of high return encourages victims to invest all they can.

When you try to withdraw large sums, the website will require more money to cover fees, taxes or to reach an arbitrary balance limit required for withdrawals. The scammer will offer to front you money to pay some of the fees. The scammer will encourage you to take on loans, mortgages, credit cards and anything they can to bleed you dry.

KEEP AN EYE OUT FOR THESE COMMON RED FLAGS:

- MESSAGES FROM STRANGERS: or people pretending to know you.
- TRANSLATION ERRORS: Many scammers are based overseas and translate their messages. Spelling and grammatical errors can be an early sign of a scam.
- ANONYMOUS MESSAGING: Strangers asking to switch from texts or social media messaging to anonymous apps like WhatsApp, Telegram, Viber, and Signal.
- NEW EXCHANGES: Regulated exchanges require you to submit Know-your-customer information like a picture of your drivers license in order to convert dollars to cryptocurrency. Scammers will require you to buy crypto through a regulated exchange, then transfer your cryptocurrency to a new exchange that they control.
- INSIDER CONNECTIONS: Scammers promise they have inside connections with trading groups, famous brokers, exchanges or trading platforms.
- TOO GOOD TO BE TRUE: If an investment seems too good to be true, it probably is. If they had such a guaranteed profit, they would go to banks, not individuals.
- TEACHING: promises to teach you how to trade in cryptocurrency options on their platform or mentor you on your journey.
- GUIDANCE: The stranger will walk you through every step, asking for screenshots to confirm you have followed instructions.
- URGENCY: The scammer will say you need invest quickly before you miss the chance.
- LARGE FEES: associated with withdrawing money from your account.
- TAXES: Americans usually do not pay taxes when they withdraw from exchanges, but the scammers will say you must pay a tax to withdraw, often at 20% or other high rates.

FOLLOW THESE TIPS TO STAY SAFE

- Do not reveal information about your personal finances or investments.
- Do not transfer, trade, or invest money with a stranger online.
- Do not share Personal Identifying Information (PII) online with strangers.
- Investigate any website or platform before entering any personal or financial information.
- Be cautious if a stranger is offering special investments or extraordinary profits. If it feels too good to be true, it probably is.

STEPS TO TAKE IF VICTIM OF A PIG-BUTCHERING SCAM

- Immediately stop transferring any money to the suspected scammer.
- Report the crime to your bank as soon as possible.
- You may need to speak with a tax professional to report the loss on your annual taxes.
- Get a police report from your local law enforcement agency.
- Contact the Georgia Secretary of State at registrations@sos.ga.gov or call (470)-312-2640.
- Contact the United States Secret Service Atlanta Field Office at https://www.secretservice.gov/ or call (404)-331-6111.
- File a report with the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/, your local FBI Field Office at https://www.fbi.gov/investigate, the Federal Trade Commission (FTC) at https://reportfraud.ftc.gov/#/#/#.