

Oregon Division of Financial Regulation warns of fake crypto apps, websites that will steal your money

December 29, 2022



The Oregon Division of Financial Regulation (DFR) warns cryptocurrency investors to do their homework before giving any money to a crypto trading platform.

Many crypto trading apps or websites are really just fake platforms set up by scammers to take investor money and give nothing in return. Investors are promised huge returns in a short amount of time and will see account balances increase rapidly, but will not be able to withdraw funds without having to deposit more money in “withdrawal fees” or “taxes.”

The scammer will continue extorting these fees until an investor becomes suspicious. After that, the account is drained and the scammers are gone, along with the investor’s funds. Before transferring money to a crypto trading website or app, research the company and web address to make sure it is legitimate.

Scammers will also look for opportunities to re-victimize those who have already been harmed and are trying to find ways to recover their losses. For example, a recent scam involved a website claiming to be managed by the U.S. Department of State, stating it was working to get FTX customer assets returned to them, following the collapse of FTX (read more about the FTX collapse).

The website asked for the investor's FTX username and password, along with other account information. The U.S. Department of State did not create this website. Please be advised that if anyone contacts you asking for usernames and passwords for your accounts, it is more than likely a scam.

"The crypto trading market is fluid and full of people trying to take advantage of you," said TK Keen, DFR administrator. "We have said this before, but if it sounds too good to be true, it probably is. We encourage everyone to do their homework and invest wisely, and be diligent in protecting their usernames, passwords, and other sensitive data."

According to the North American Securities Administrators Association, there are many common schemes fraudsters exploit as new investment products or opportunities. Some of them are:

- **Fake digital wallets:** A digital wallet is used to store, send, and receive cryptocurrencies. Scammers design a fake digital wallet to lure users into providing their private key or code that enables the wallet to open. Once scammers receive the private key, they can steal all the cryptocurrency from the owner's digital wallet.
- **Pump-and-dumps:** Groups of individuals coordinate to buy a thinly-traded cryptocurrency, promote the cryptocurrency on social media to push up demand and the price, and then sell it in a coordinated sale. The price plummets and those unaware of the scheme are left with the devalued cryptocurrency.
- **Multi-level marketing platforms:** Companies lure investors through the promise of high interest with low risk. These investors are then incentivized to recruit more members.

"Many of these seem obvious after the fact, but there is so much in this industry that looks and sounds legitimate," Keen said. "Unfortunately, there are a lot of people out there in the crypto space who are just looking to take advantage of you. If you think you are a victim of a crypto-related scam, we encourage you to file a complaint with our office."

For more information on filing a complaint, go to the DFR website.

###

About Oregon DFR: The Division of Financial Regulation is part of the Department of Consumer and Business Services, Oregon's largest business regulatory and consumer protection agency. Visit dfr.oregon.gov and www.dcbbs.oregon.gov.