ripple

How to Spot and Report Crypto Scams

You may have seen them: the social media posts from scammers posing as President Joe Biden, Elon Musk and other public figures promising free cryptocurrency. These posts include branding and profile pictures that look exactly like what the companies, individuals or government authorities use. It's important to be able to spot which accounts are fake, and which posts are scams.

Scams like these exploit high-profile social media accounts to trick followers into enriching the scammers at the targets' expense. These scams can manifest in many forms, including: fraudulent investment and business opportunities, crypto giveaway promises, fake job offers, blackmail emails and even online dating.

These scams are an unfortunate byproduct of cryptocurrency becoming more mainstream and are a very real concern with high-priced repercussions. As the International Association of Better Business Bureaus reports, the number of victims of cryptocurrency giveaway scams nearly tripled from 2019 to 2021.

And while cryptocurrency scams remain a small fraction of overall fraud,concerned regulators, industry players and advocates are taking proactive steps to help prevent surges in social media scams and aid in consumer protection, regardless if they use crypto or not.

Since Ripple's founding, we and others have requested the removal of countless fake ads and posts that promise the giveaway of free XRP—an open-source, decentralized cryptocurrency built for cross-border payments. As a trusted resource in a growing industry where trust is paramount, it's important to us to help educate consumers about these threats and how to avoid them. In support of this, here is a list of authentic social media handles of Ripple corporate accounts and some of Ripple's executives:

- X (formerly Twitter)
  - @Ripple
  - @RippleXDev and @RippleDevRel
  - Brad Garlinghouse @bgarlinghouse
  - Stu Alderoty @s_alderoty
  - Monica Long @MonicaLongSF
  - David Schwartz @JoelKatz
- Ripple LinkedIn
- Ripple Instagram @ripple_global
- Ripple Facebook
- Ripple YouTube

What's Real vs. What's Not

Social media has enabled misinformation to spread quickly, so it's more important than ever to be aware and vigilant of what's real and what's not. Data from 2021 shows $2.3b worth of losses due to imposter scams were reported — a $1.1b increase from the prior year — while social media scams have cost consumers $2.7b between 2021 and 2023

Some scammers impersonate companies and individuals by posting images on social media platforms like Twitter, Facebook, or Instagram. Others use legitimate videos from media interviews or public speaking events and overlay scam content that may link to a fraudulent website or a crypto wallet address asking targets to send money.

We've seen an uptick in 2023 of scammers digitally manipulating videos (known as "deepfakes") to develop convincing hoaxes by using the likeness of a public figure. Because deepfakes can be difficult to identify, they have contributed to the spread of misinformation, crypto scams and other fraudulent acts.

More often than not, these posts will lead to fraudulent web domains with a public "send to" wallet address. There may even be a chat feature on the website to quickly convince you to send over valuable digital assets.

Always err on the side of caution when asked to share financial information, even if it seems to be coming from a reputable source or someone you know personally.

How to Spot Giveaway Scams
Here are some helpful tips for spotting and reporting these harmful giveaway scams.

- In many cases, the first warning that a giveaway ad is a scam is that **in order to receive the reward, you must first send money** and/or provide your personal financial account information. For any real sweepstakes, winnings are always free and never ask for money or financial account information upfront.

- Impersonations are more challenging to spot—often because scammers create a sense of legitimacy by using logos, social media verification checks, company executive social handles, profile images, graphics, deepfakes or legitimate video excerpts with branding that match real corporate imagery. **Personal due diligence is key here.**

- If a giveaway looks real, **visit the company's website and verified social channels to confirm if the ad exists** there as well. You can even contact the company directly and inquire about the contest to verify authenticity.

- Additionally, scammers will leverage legitimate accounts to falsify a sense of proof by commenting on top of social posts with fake accounts. Some other quick **visual signs that a commenting account might be a scam is the lack of a profile picture, odd account names, or terminology in the comment that "loves" or "thanks" the company for the giveaway winnings.**

Taking Action Against Crypto Scams

Reporting suspicious behavior can often turn into a game of Whac-a-mole. As soon as one scam is reported and removed, a new scam quickly replaces it. The reporting of these scams largely relies on the company involved as well as social media users (the targets) to identify and request removals of fake accounts and harmful giveaway scams.

If you suspect you've come across a crypto scam, you can report fraud and other suspicious activity involving cryptocurrency to the Federal Bureau of Investigation (FBI). For fraudulent website reporting, use this quick form to submit the URL to Google which may be escalated to a third party for further investigation.

In response to the numerous XRP giveaway scams and impersonations, Ripple has also hired an external cybersecurity and digital threat intelligence vendor to help with reporting and takedown efforts. We also encourage using "Google Safe Browsing" which will warn users of dangerous websites or downloads.

At the end of the day, where there is money, there are always those looking to steal it. So it's vital to be mindful of what you see on social media, to be on the lookout for signs of crypto scams and, most importantly, to protect yourself. No more crypto community members or global consumers need to fall victim to these harmful scams. Remember, we're all in this together.

The availability of Ripple's products and services and their respective features varies by jurisdiction.
©Copyright Ripple November 2023. All rights reserved.