What are the most prevalent crypto scams to be aware of?

10/07/2024 8:56 pm EDT

The most common crypto scams we encounter on a day-to-day basis include:

1. Pig Butchering Scams -- Pig butchering scams specifically target users that have little to no knowledge of cryptocurrency. The scammer takes a while to build up rapport and a relationship with the victim so that the victim trusts them. The scammer then directs or 'recommends' the victim start using a [fraudulent] investment platform, and helps 'coach' the victim. A considerable portion of the time, the scam comes about due to a romantic connection found on an online dating app such as Hinge.

2. Job / Employment Scams -- They require victims to put up some of their own money for tools/onboarding/capital, and are sometimes given menial tasks to a 'job'

3. Phishing scams - phishing comes in many different shapes, colors, and forms. Some of the most frequent types of phishing scams to be aware of

a) Phishing scams attempting to have the user provide their seed phrase or private keys. This can be through a malicious application, fraudulent website, or malicious email a user may receive as a result of a database breach

b) Drainers & Malicious Smart contracts -- Phishing attacker often try to get victims to approve malicious smart contracts designed to drain a victims wallet of funds. The attacker does not need the seed phrase or private key to do this. Victims encounter drainers from a variety of sources, including blog articles (that are purporting to be helpful), and malicious airdrops, to name but a couple common sources.

4. Impersonation Scams -- Impersonation scams are still incredibly common, and include things like fake customer support reps and fake community managers