Stay Safe

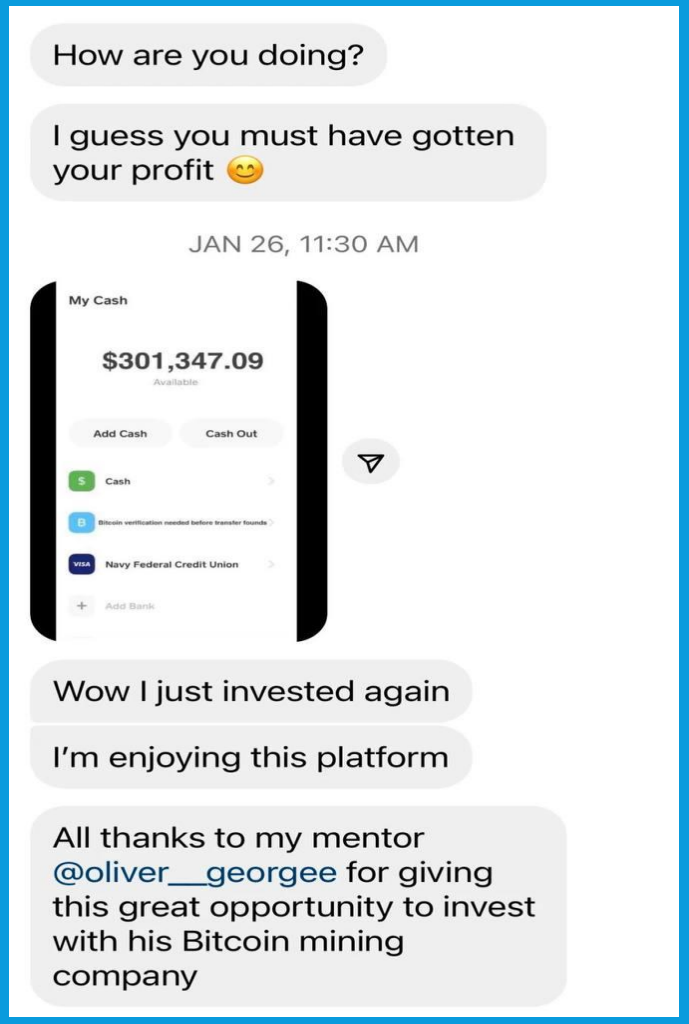
Common Crypto Scams

1. BITCOIN INVESTMENT SCHEMES

- In bitcoin investment schemes, scammers contact investors claiming to be seasoned "investment managers." As part of the scheme, the so-called investment managers claim to have made millions investing in cryptocurrency and promise their victims that they will make money with investments.

- To get started, the scammers request an upfront fee. Then, instead of making money, the thieves simply steal the upfront fees. The scammers may also request personal identification information, claiming it's for transferring or depositing funds, and thus gain access to a person's cryptocurrency.

- Another type of investment scam involves using fake celebrity endorsements. Scammers take real photos and impose them on fake accounts, ads or articles to make it appear as though the celebrity is promoting a large financial gain from the investment. The sources for these claims appear to be legitimate, using reputable company names such as ABC or CBS with a professional-looking website and logos. However, the endorsement is fake.



2. RUG PULL SCAMS

- Rug pull scams involve investment scammers "pumping up" a new project, nonfungible token (NFT) or coin to get funding. After the scammers get the money, they disappear with it. The coding for these investments prevents people from selling the bitcoin after purchase, so investors are left with a valueless investment.

- A popular version of this scam was the Squid coin scam, named after the popular Netflix series *Squid Game*. Investors had to play to earn cryptocurrency: People would buy tokens for online games and earn more later to exchange for other cryptocurrencies. The price of the Squid token went from being worth 1 cent to about $90 per token.

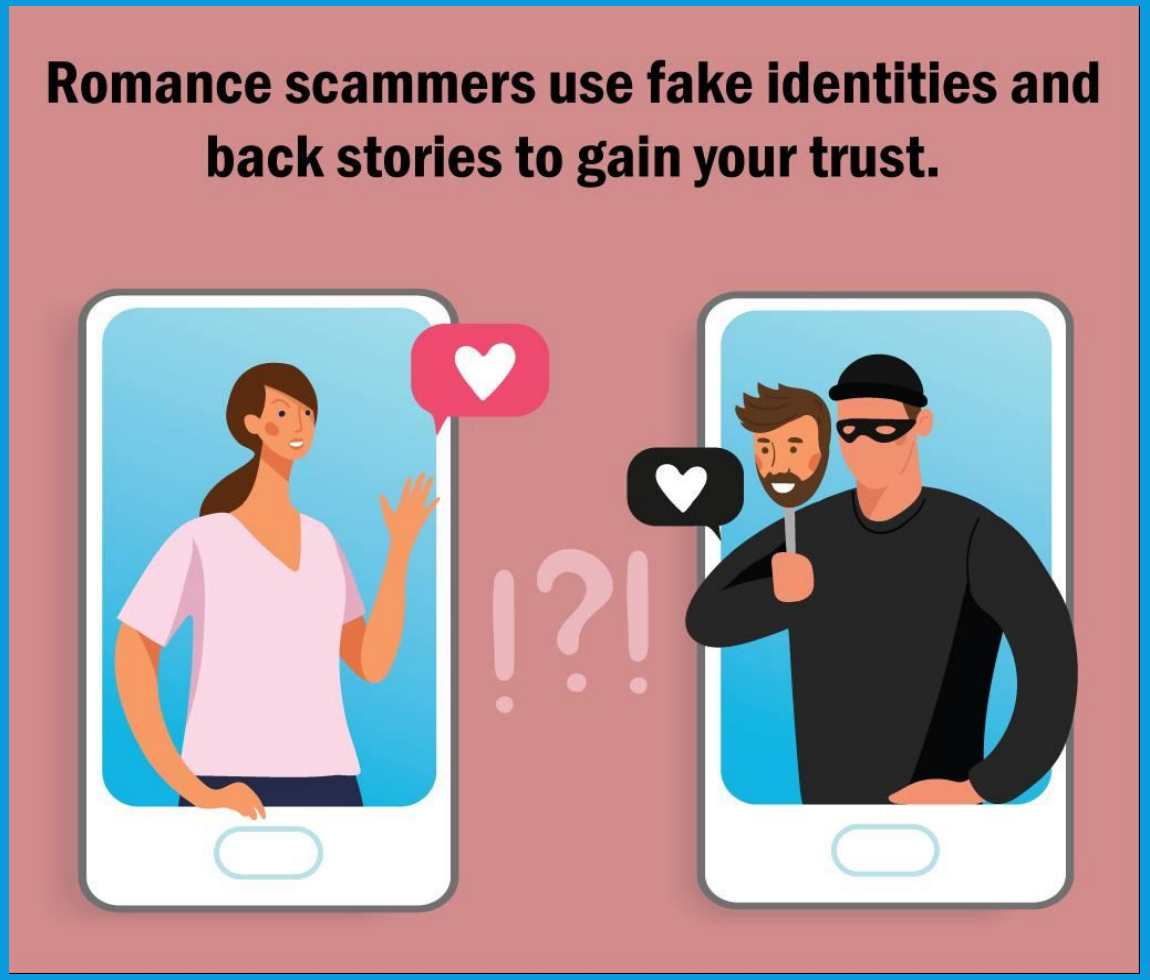
- Eventually, trading stopped and the money disappeared. The token value then reached zero as people attempted but failed to sell their tokens. The scammers made about $3 million from these investors.

- Rug pull scams are also common for NFTs, which are one-of-a-kind digital assets.

3. ROMANCE SCAMS

- Dating apps are no stranger to crypto scams. These scams involve relationships -- typically long-distance and strictly online -- where one party takes time to gain the other party's trust. Over time, one party starts to convince the other to buy or give money in some form of cryptocurrency.

- After getting the money, the dating scammer disappears. These scams are also referred to as "pig butchering scams."



4. PHISHING SCAMS

- Phishing scams have been around for some time but are still popular. Scammers send emails with malicious links to a fake website to gather personal details, such as cryptocurrency wallet key information.

- Unlike passwords, users only get one unique private key to digital wallets. But if a private key is stolen, it is troublesome to change this key. Each key is unique to a wallet; so, to update this key, the person needs to create a new wallet.

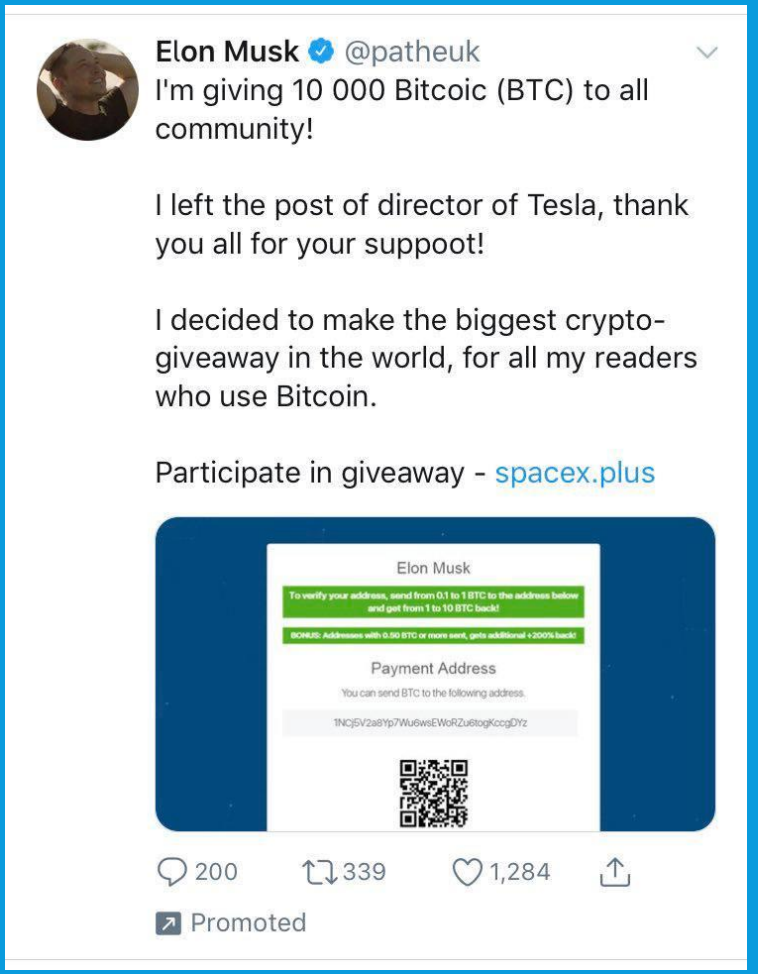
- To avoid phishing scams, never enter secure information from an email link. Always go directly to the site, no matter how legitimate the website or link appears.

5. SOCIAL MEDIA CRYPTOCURRENCY GIVEAWAY SCAMS

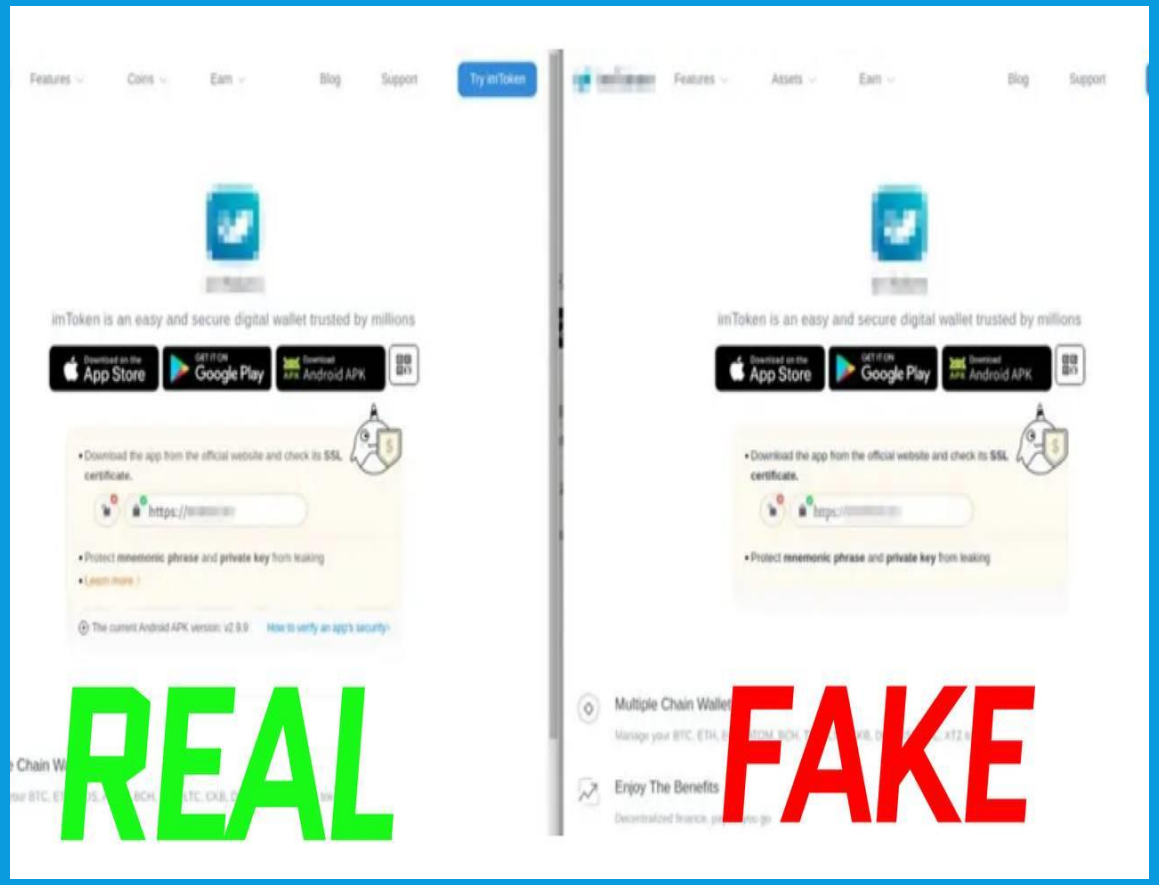
- There are many fraudulent posts on social media outlets promising bitcoin giveaways. Some of these scams also include fake celebrity accounts promoting the giveaway to lure people in.

- However, when someone clicks on the giveaway, they are taken to a fraudulent site asking for verification to receive the bitcoin. The verification process includes making a payment to prove the account is legitimate.

- The victim can lose this payment -- or, worse yet, click on a malicious link and have their personal information and cryptocurrency stolen.



8. FAKE CRYPTOCURRENCY EXCHANGES



- Scammers may lure investors in with promises of a great cryptocurrency exchange -- maybe even some additional bitcoin. But in reality, there is no exchange and the investor does not know it's fake until after they lose their deposit.

- Stick to known crypto exchange markets -- such as Coinbase, Crypto.com and Cash App -- to avoid an unfamiliar exchange. Do some research and check industry sites for details about the exchange's reputation and legitimacy before entering any personal information.

HOW TO PROTECT BITCOIN AND CRYPTOCURRENCY

To protect against cryptocurrency scams, here are some of the common red flags:

- **promises for large gains or double the investment;**
- **only accepting cryptocurrency as payment;**
- **contractual obligations;**
- **misspellings and grammatical errors in emails, social media posts or any other communication;**
- **manipulation tactics, such as extortion or blackmail;**
- **promises of free money;**
- **fake influencers or celebrity endorsements that seem out of place;**
- **minimal details about money movement and the investment; and**
- **several transactions in one day.**