CRYPTO SCAMS

AND HOW TO AVOID THEM

The rise in popularity of cryptocurrencies has encouraged cybercriminals to find innovative ways to attack markets, users and any structure where cryptocurrencies are stored. In simple words, if an attacker is able to exploit some area of a chain, smart contract, exchange or illegitimately withdraw cryptocurrency, it would be deemed as a hack or stealing. Scammers around the world took home a record of $14 billion in cryptocurrency in 2021.

MALWARE

Malware refers to malicious software that carries out harmful activity on a victim's device, usually without their knowledge. Malware-powered crime can be as simple as stealing information or money from victims, but can also be much more complex and grand in scale.

- **NEVER RUN OR OPEN UNKNOWN FILES ON YOUR DEVICE**
  Always double-check files before you run them on your device. You can use services like virustotal to make sure that file is safe.
- **DON'T BLINDLY TRUST EMAIL ATTACHMENTS**
  Email attachments can infect your computer with dangerous malware or ransomware - that will encrypt all of your files.

PHISHING

Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, crypto wallet details through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

- **GOOGLE ADS PHISHING**
  There has been a huge increase in the number of Google phishing ads.
- **LOOK-ALIKE DOMAINS**
  Pay attention to fake domain TLD metamask.**gr** or trezor.**us.**
- **EMAIL SPOOFING**
- **SOCIAL MEDIA CLONES**
- **BEWARE OF REDIRECTIONS AND URL SHORTENERS**

https://alvosec.com/dont-feed-the-phish/

FAKE SUPPORT

There are groups pretending to be the support team of a company in order to access private and sensitive information, like wallet password or private keys.

- **FAKE TOKEN PRESALE**
  Anyone can create and name token especially creating a fake version of existing token to influence presale.
- **FAKE WALLETS**
- **FAKE EXCHANGE**
  Example of QuadrigaCX where owner stole over $200 million of customer assets.

SOCIAL MEDIA SCAMS

There are thousands of scam social accounts with misleading information about giveaway and potential cryptocurrency ponzi schemes. Double check authenticity of any social media account!

SOCIAL ENGINEERING ATTACKS

Exploiting the Human Factor: Social engineering targets especially the users of a system. It is increasingly being applied to cryptocurrency users. Read our blog to detect early stage of social engineering attacks.

https://alvosec.com/what-is-social-engineering/

One single vulnerability is all an attacker needs!

ALVOSEC
PROTON BLOCK PRODUCER

VOTE FOR US

ABOUT ALVOSEC

We are primarily focused to provide greater security for the ecosystem itself and for all Proton users. As you may already know Alvosec is part of HackerOne since 2017, where thousands of hackers have tried to break our systems. Through similar platforms we gained knowledge and experience to develop a strategy against early stage attacks. Our mission in Proton chain will be to advise in implementing stronger security practices and raise security awareness for entire community. We have already launched a honeypot that will trap attackers and monitor their activities to enhance network security.

https://alvosec.com