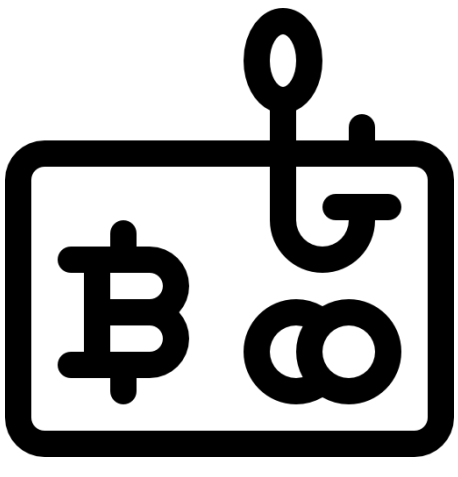
A CRYPTO CRIME

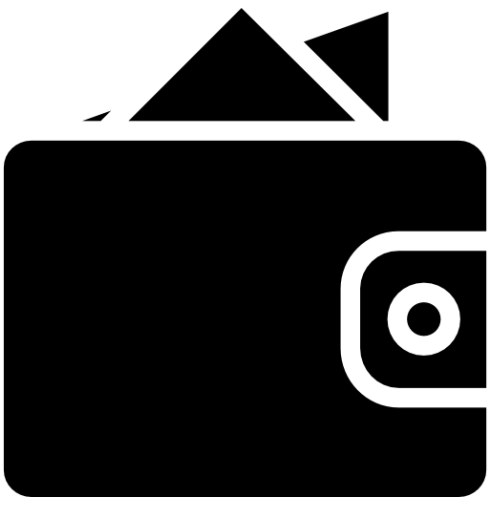
CRYPTO PHISHING



PAST

2009-PRESENT

The increase in value of cryptocurrencies forced criminals to reconsider their traditional phishing attacks. With the advent of cryptocurrencies and related technology, attackers now had a new target set in their sights, crypto assets.

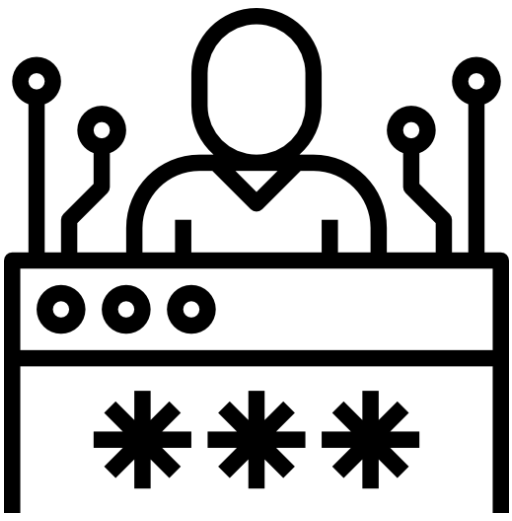


PRESENT

2018

Crypto Phishing Has Evolved In The Following Ways:

- Increased use of social media to facilitate attacks
- Attackers are focusing on high value cryptocurrencies
- SMS and chat applications are also being used
- Attackers are spending money on advertising to increase the success of their attacks
- Crypto phishers are buying up domains related to cryptocurrency wallet and exchange sites



FUTURE

2018+

Crypto Phishing Predictions For The Future:

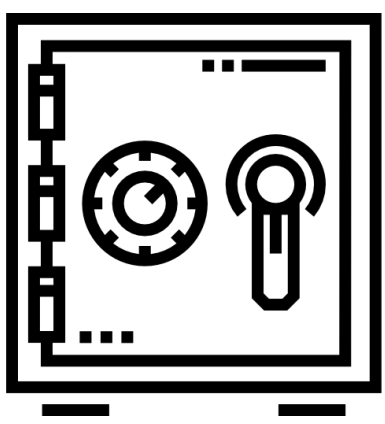
- Attackers using fake social media community pages to launch attacks on members of the real community
- Malicious actors will invest more time and effort into these attacks because of the potential return
- Users of a specific cryptocurrency will be targeted

VULNERABILITIES

- Uneducated users
- Weak email security
- Lack of policy and direction
- Allowing more people to be able to access or control your crypto assets than is absolutely necessary.

MITIGATION

- Block spam and email in languages from countries you do not do business with
- Educate users about phishing threats
- Ensure you are visiting the correct site
- Keep you keys in the most secure place possible
- Protect your credentials at all costs
- Do not trust emails that manipulate human weaknesses such as: the fear of missing out, ego, superiority, etc.



THE SECURITY STRONGHOLD

https://thesecuritystronghold.com

contact@thesecuritystronghold.com

+ (1) 715-347-8979