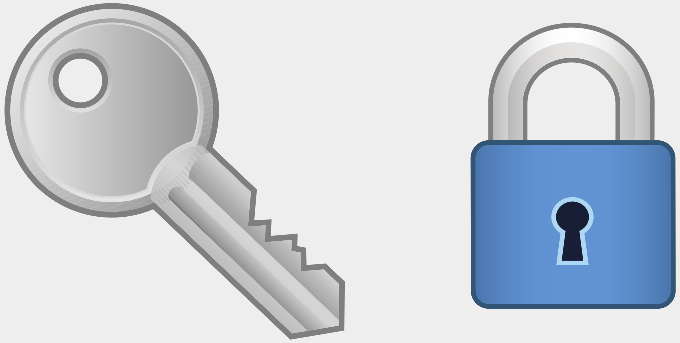
Talking to Your Users About Cryptocurrency Security

A Little About Me...

- Software Engineer @ Microsoft in Pittsburgh
- Tech Educator @ chaintuts
- Love to build free and open source technical education!
  - Interested in cryptocurrencies, blockchains, digital security topics

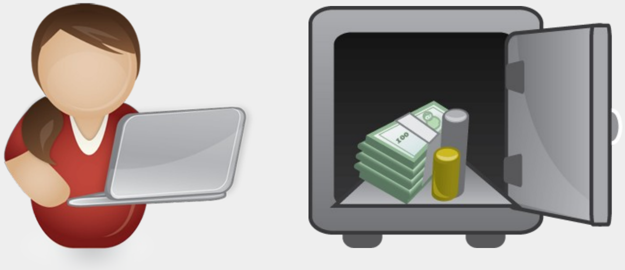
The Core of Crypto Ownership: Private Keys

- We call a cryptocurrency private key store a *wallet*
- It’s absolutely critical that wallets (private keys) are both:
  - Securely *generated*
  - Securely *stored*
- There are different *classes* of wallets, all with differing threats



Wallet Security Overview

- Much of this may not be news to technical & security pros
- We as the builders have a duty to educate our users on security
- Want to give you new ways to think about *security education* for cryptocurrencies



Discussing Security

- *Classes* wallets, and broad security overview
- Common cryptocurrency threats
- Security bullet-points for your users

Wallet Class Security Overview

Most secure (non-custodial)

Least secure (non-custodial)

Security varies (custodial)

- Offline wallets
- Online mobile wallets
- Online desktop wallets
- Online web wallets

- Exchanges (special case)

Wallet Class Security Overview

- Broadly speaking:
  - Offline is better than online
  - Specialized hardware is better than general purpose
  - Self-custody is better than an exchange -
    - IF the user is prepared for it (special case)
  - *The amount will dictate the level of security needed*

Hardware/Offline Wallets

- Users should be highly encouraged to use *hardware wallets*
- All key generation and storage is done *offline* on *specialized hardware*
- Greatly lowers the attack surface for key theft!
  - Can’t watch keygen, signatures (key leakage)
  - Can’t phone home with stolen keys
  - Can’t run gen-purpose malware

```
Address:
1KULHaNZafvGCRrVLfWw
VfQjXh7x9dASa9
```

My demo DIY hardware wallet
uBitAddr

Online Wallets

- For online use, encourage *mobile applications* over desktop, web wallets
- Mobile has more locked-down OS
  - Less susceptible to malware, but not foolproof
  - Most users go through app stores, which have some safeguards in place

Online Wallets

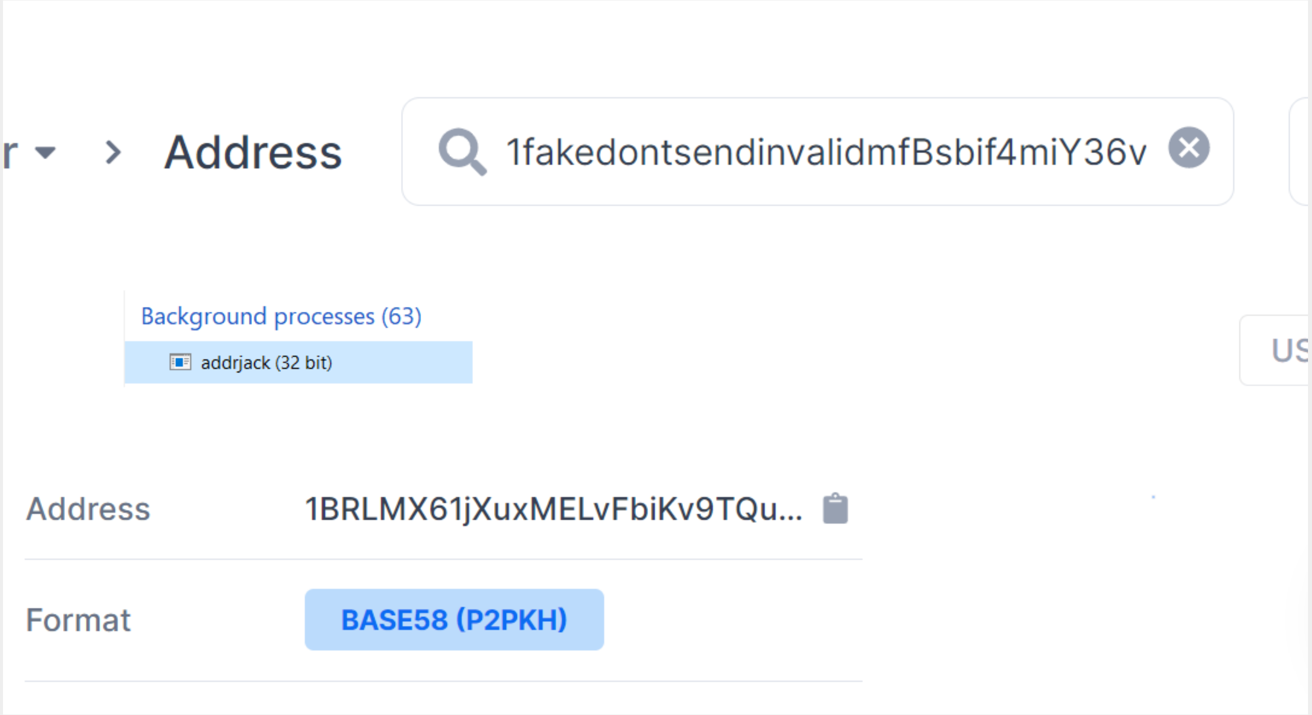
- Desktop and web wallets present the *highest attack surface* – discourage
  - Malware threats
  - Key leakage/theft
  - Phishing attacks
  - Bad passwords, password reuse

Exchanges

- Exchanges are a special case, because:
  - You are trusting a “Bitcoin bank” instead of holding keys yourself
  - Security is only as good as:
    - Their security (which is a big target)
    - Your password, 2FA hygiene

Let’s Talk Threats #1

- Malware threats (desktop, web, mobile)
  - Address jacking (demo: AddrJack)
  - Fake wallet software (ex: fake Electrum updates)
  - Key theft malware



1fakedontsendinvalidmfBsbif4miY36v

Background processes (63)

addrjack (32 bit)

Address 1BRLMX61jXuxMELvFbiKv9TQu...

Format BASE58 (P2PKH)

Let’s Talk Threats #2

- Bad passwords and 2FA hygiene (web, exchanges)
  - People love to reuse passwords...this is particularly dangerous for web wallets and exchange accounts
  - Most people don’t use long, higher entropy passphrases (*length over complexity!!*)
  - SMS based 2FA is vulnerable to SIM-swap attacks
  - Users may skip 2FA altogether

Let’s Talk Threats #3

- Phishing & Social Engineering (*Everything)*
  - The absolute hardest to protect your users from…
  - “Fake investment (forex, mining, etc.)” scams
  - “Fake giveaway scams”
  - Ledger data breach related scams – extortion, fake software updates, etc.
  - **Most thefts I have seen happen through social engineering, *not* technical exploits!**

Bullet Points for Your Users

- Encourage *hardware wallets* for high-value accounts
- Encourage *mobile wallets* for spending money
- Encourage/require *strong passphrases* (length over complexity) for wallets, exchanges
- Encourage/require *strong app or hardware based 2 factor authentication*
- ***Train your users on social engineering!***

Bullet Points for Your Users

- Security landscape is ever evolving
- This is not a comprehensive list – be open to new info and feedback
- With great power (being your own bank) comes great responsibility
- **Overall:**
  - **Train your users to think about security first!**
  - **Develop software with security-first mindset!**

Questions?