Subtle and not so Subtle Ways to Lose Your Cryptocurrency

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
    - Tired of meeting folks **after** they lost money – I want to help people *before* that happens

Cryptocurrency – Powerful But Vulnerable….

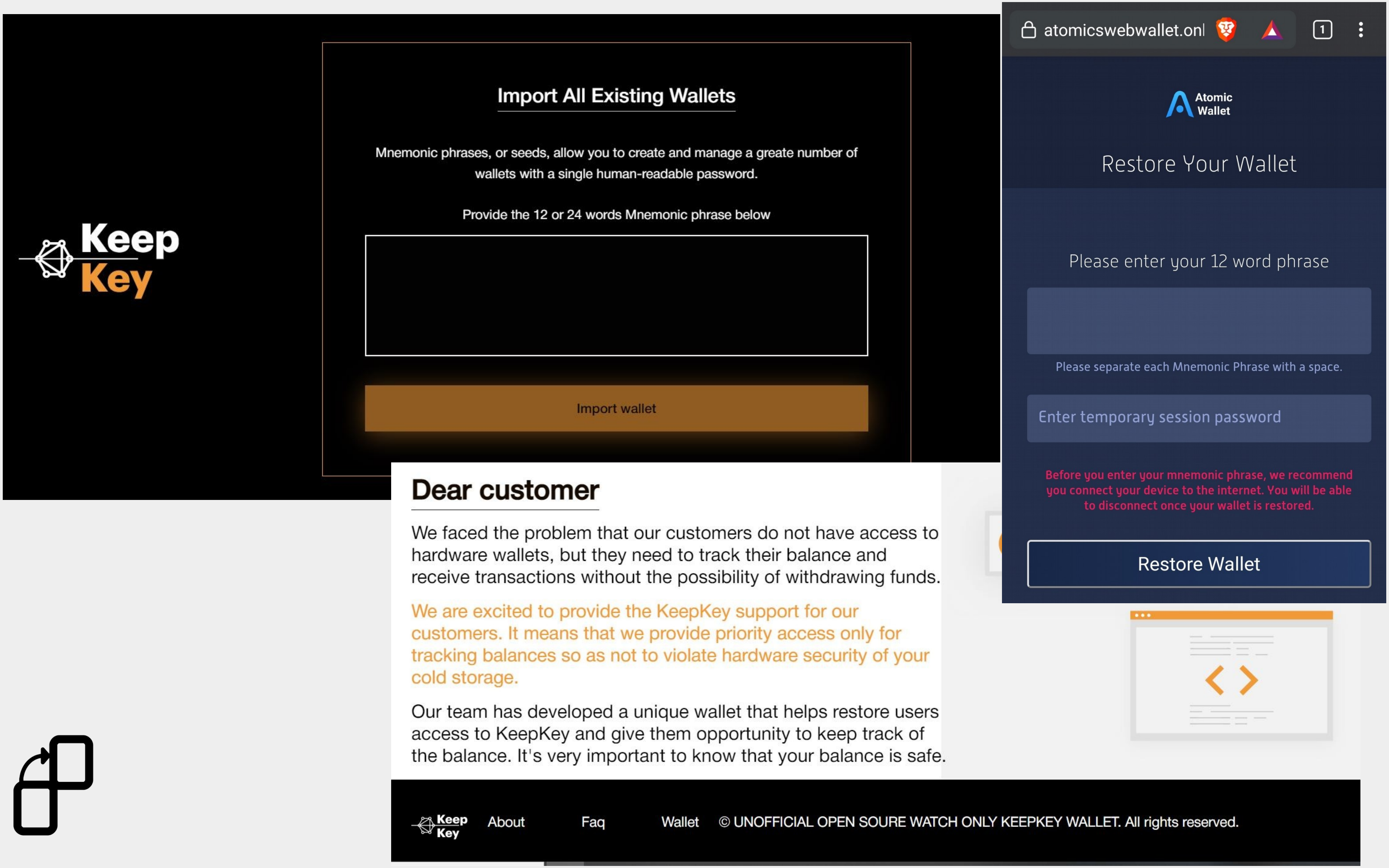
- Cryptocurrencies are powerful tools with irreversible transactions and PKI
- Thieves and scammers take advantage of this
- What you’ll get:
  - Common attack vectors & mitigation techniques
  - **Take this back to your products, users, etc.!**

Cryptocurrency – Powerful But Vulnerable….

- Social Engineering
- Malware
- User Error
- Bad Security Hygiene Practices
- Wallet Implementation Problems

… all ways *real* users get rekt. Let’s talk about fixing that!

Social Engineering #1 – Fake “Support”



Import All Existing Wallets

Mnemonic phrases, or seeds, allow you to create and manage a greate number of wallets with a single human-readable password.

Provide the 12 or 24 words Mnemonic phrase below

Restore Your Wallet

Please enter your 12 word phrase

Please separate each Mnemonic Phrase with a space.

Enter temporary session password

Before you enter your mnemonic phrase, we recommend you connect your device to the internet. You will be able to disconnect once your wallet is restored.

Dear customer

We faced the problem that our customers do not have access to hardware wallets, but they need to track their balance and receive transactions without the possibility of withdrawing funds.

We are excited to provide the KeepKey support for our customers. It means that we provide priority access only for tracking balances so as not to violate hardware security of your cold storage.

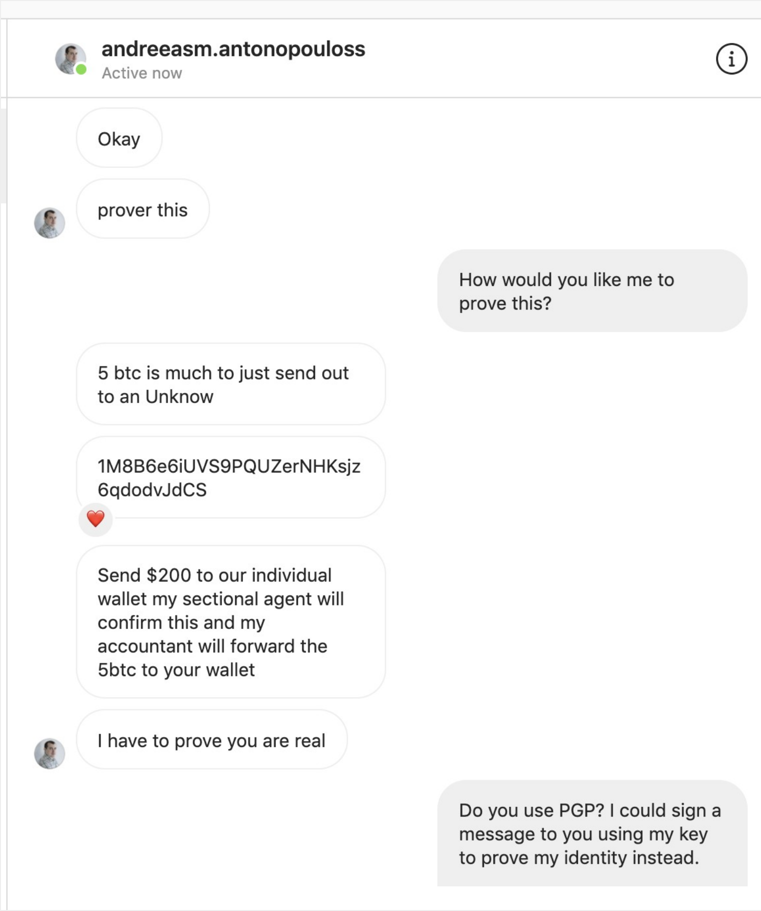
Our team has developed a unique wallet that helps restore users access to KeepKey and give them opportunity to keep track of the balance. It's very important to know that your balance is safe.

© UNOFFICIAL OPEN SOURE WATCH ONLY KEEPKEY WALLET. All rights reserved.

Social Engineering #1 – Fake “Support”

- Example #1 - Crypto company "support" phishing - ex: fake KeepKey wallet tools
- **Attack:** trick the user into giving up account access (via 2FA codes/password reset) or seed phrase (direct access to keys)
- **Countermeasures:** Know that no legitimate support will ask for 2FA codes, seed phrases
    - We need warnings on our stuff; reminders for end users

Social Engineering #2 – Impersonation



andreeasm.antonopouloss
Active now

Okay

prover this

How would you like me to prove this?

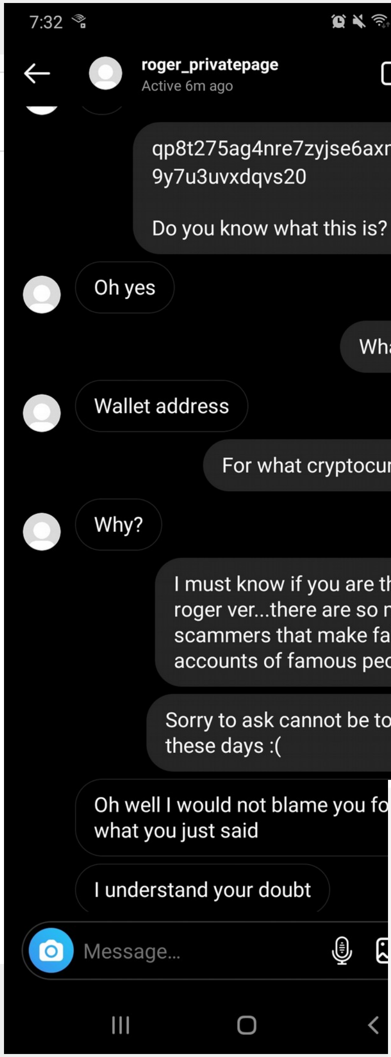
5 btc is much to just send out to an Unknow

1M8B6e6iUVS9PQUZerNHKsjz6qdodvJdCS

Send $200 to our individual wallet my sectional agent will confirm this and my accountant will forward the 5btc to your wallet

I have to prove you are real

Do you use PGP? I could sign a message to you using my key to prove my identity instead.



7:32 52%

roger_privatepage
Active 6m ago

qp8t275ag4nre7zyjse6axmg5y8t9y7u3uvxdqvs20

Do you know what this is?

Oh yes

What is it?

Wallet address

For what cryptocurrency?

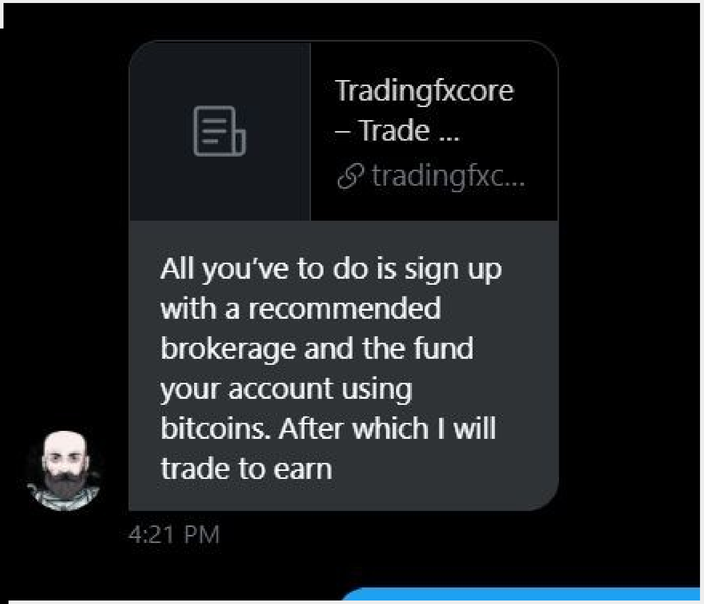
Why?

I must know if you are the true roger ver...there are so many scammers that make fake accounts of famous people

Sorry to ask cannot be too safe these days :(

Oh well I would not blame you fo what you just said

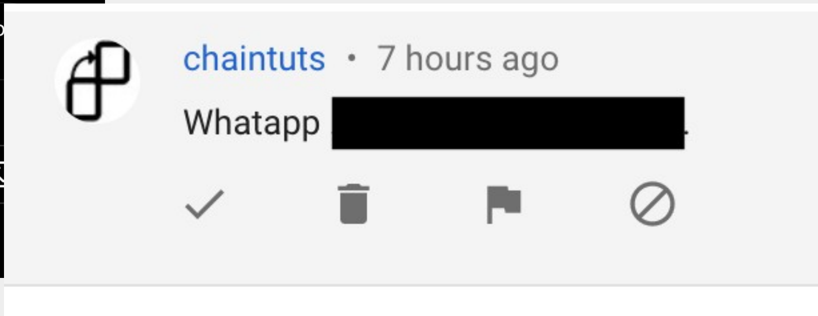
I understand your doubt



Tradingfxcore – Trade ...
tradingfxc...

All you've to do is sign up with a recommended brokerage and the fund your account using bitcoins. After which I will trade to earn

4:21 PM



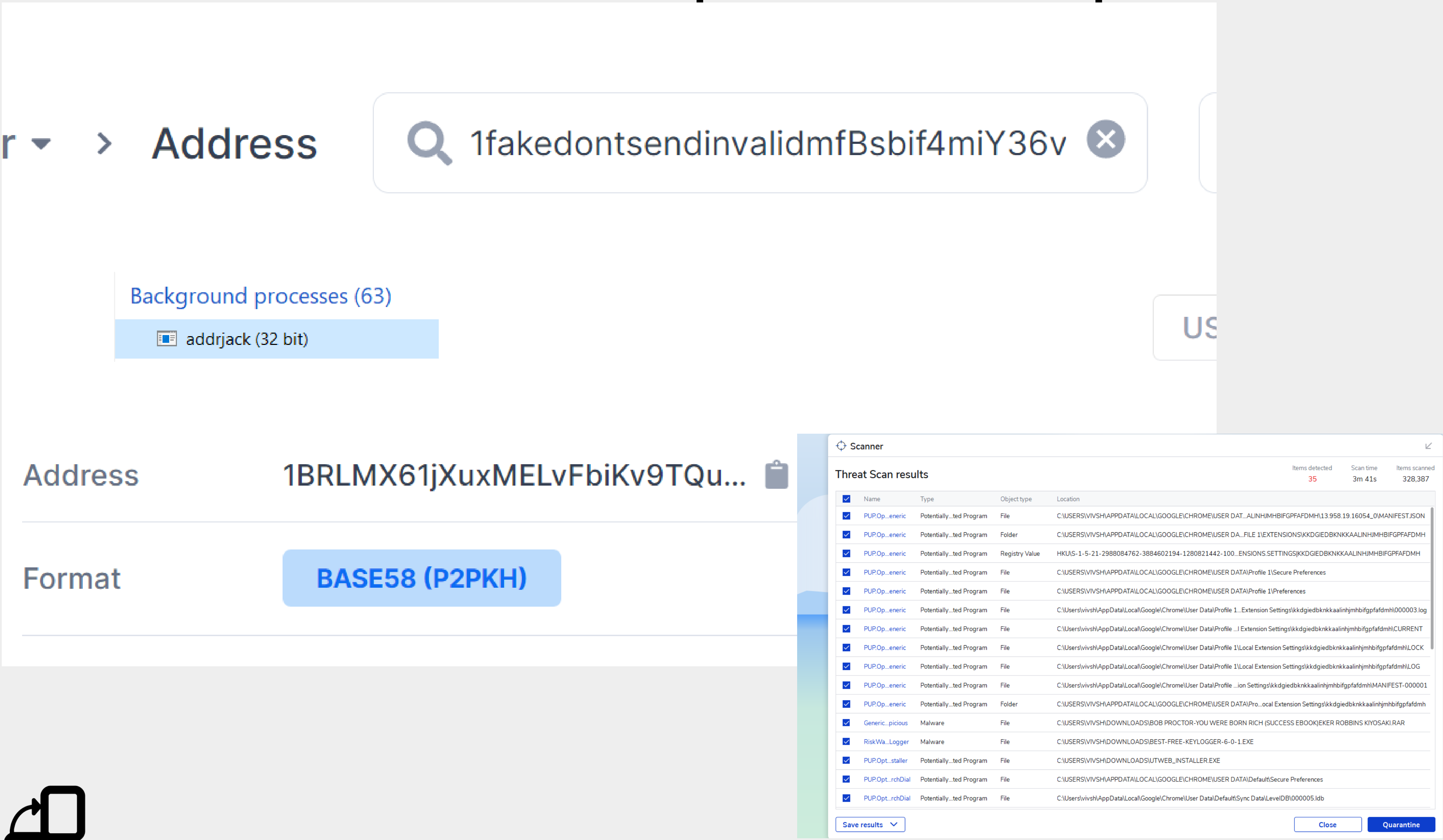
chaintuts • 7 hours ago

Whatapp [redacted]

Social Engineering #2 – Impersonation

- Example #2 – Impersonation ex: fake Andreas, Roger, chaintuts, etc.
- **Attack:** an account impersonating a crypto celebrity tricks you into sending Bitcoin to a fake, but convincing "Bitcoin investment" website
- **Countermeasures:** awareness of the irreversibility of crypto transactions, what these scams look like, impersonation tactics
  - Ex: Andreas' Twitter bio says "BEWARE of giveaway scams" - a simple message goes a long way

Malware – Clipboard Swaps



Background processes (63)

addrjack (32 bit)

Address 1BRLMX61jXuxMELvFbiKv9TQu...

Format BASE58 (P2PKH)

Scanner

Threat Scan results

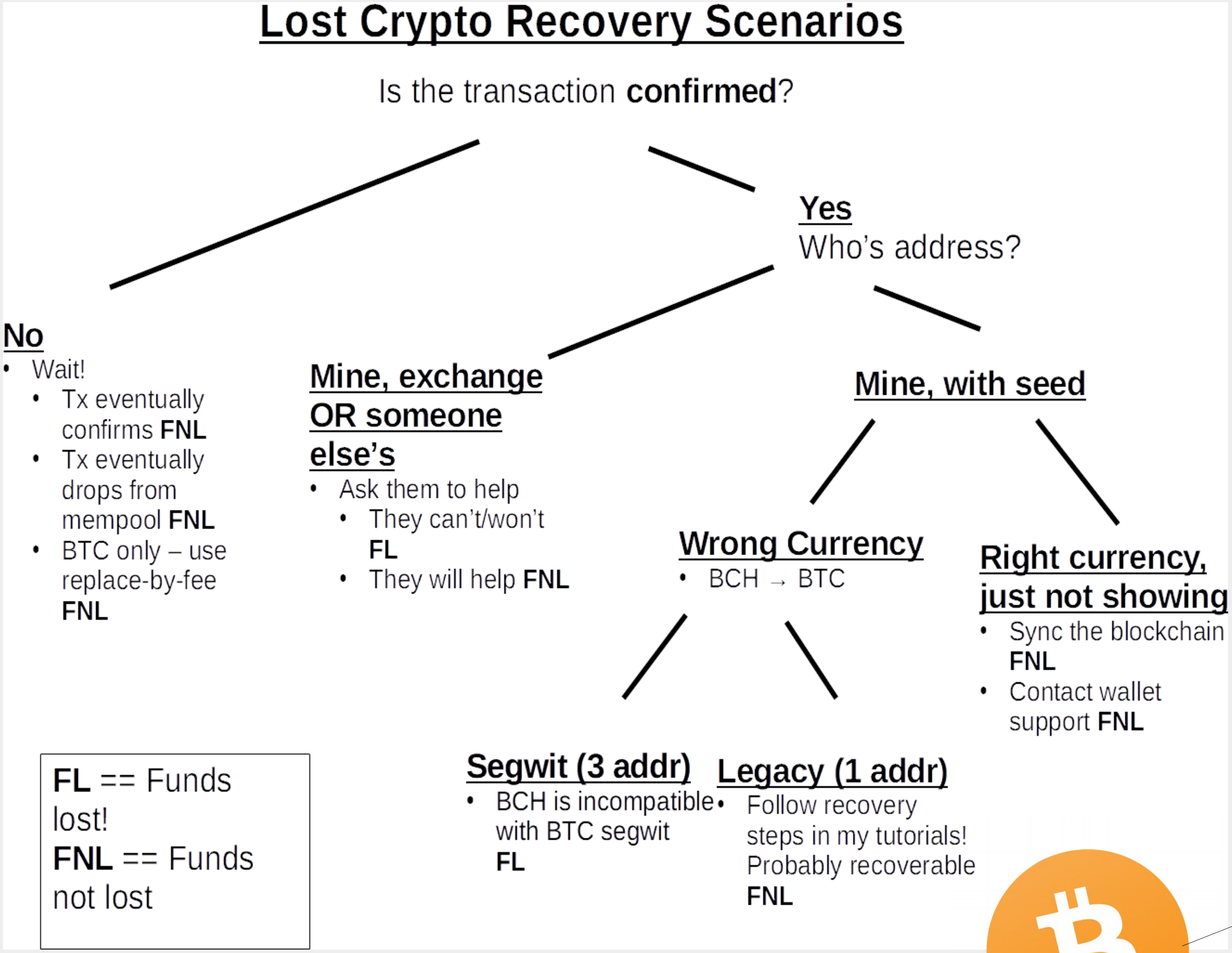
Items detected	Scan time	Items scanned
35	3m 41s	328,387

☑	Name	Type	Object type	Location
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DAT...ALINHJMHBIFGPFAFDMH\13.958.19.16054_0\MANIFEST.JSON
☑	PUP.Op...eneric	Potentially...ted Program	Folder	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DA...FILE 1\EXTENSIONS\KKDGIEDBKNKKAALINHJMHBIFGPFAFDMH
☑	PUP.Op...eneric	Potentially...ted Program	Registry Value	HKU\S-1-5-21-2988084762-3884602194-1280821442-100...ENSIONS.SETTINGS|KKDGIEDBKNKKAALINHJMHBIFGPFAFDMH
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\Profile 1\Secure Preferences
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\Profile 1\Preferences
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Profile 1...Extension Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh\000003.log
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Profile ...l Extension Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh\CURRENT
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh\LOCK
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Profile 1\Local Extension Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh\LOG
☑	PUP.Op...eneric	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Profile ...ion Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh\MANIFEST-000001
☑	PUP.Op...eneric	Potentially...ted Program	Folder	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\Pro...ocal Extension Settings\kkdgiedbknkkaalinhjmhbifgpfafdmh
☑	Generic...picious	Malware	File	C:\USERS\VIVSH\DOWNLOADS\BOB PROCTOR-YOU WERE BORN RICH (SUCCESS EBOOK)EKER ROBBINS KIYOSAKI.RAR
☑	RiskWa...Logger	Malware	File	C:\USERS\VIVSH\DOWNLOADS\BEST-FREE-KEYLOGGER-6-0-1.EXE
☑	PUP.Opt...staller	Potentially...ted Program	File	C:\USERS\VIVSH\DOWNLOADS\UTWEB_INSTALLER.EXE
☑	PUP.Opt...rchDial	Potentially...ted Program	File	C:\USERS\VIVSH\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\Default\Secure Preferences
☑	PUP.Opt...rchDial	Potentially...ted Program	File	C:\Users\vivsh\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000005.ldb

Malware – Clipboard Swaps

- Example – my homebrew “AddrJack”
  - Https://github.com/chaintuts/addrjack
  - https://youtu.be/suOpeSUlwN8 - Quick demo
  - It takes all of 30 minutes to make a basic one, and real ones are more sophisticated!
- **Attack:** malware on a user's computer senses a crypto address in the clipboard, swaps it to an attackers. The user pastes the malicious address and sends coins to the attackers
- **Countermeasures:** Always double, triple checking that addresses match the intended recipient’s

User Error #1 – “Cross Chain” Swaps



Lost Crypto Recovery Scenarios

Is the transaction **confirmed**?

No

- Wait!
  - Tx eventually confirms **FNL**
  - Tx eventually drops from mempool **FNL**
  - BTC only – use replace-by-fee **FNL**

Yes
Who’s address?

Mine, exchange OR someone else’s

- Ask them to help
  - They can’t/won’t **FL**
  - They will help **FNL**

Mine, with seed

Wrong Currency

- BCH → BTC

Right currency, just not showing

- Sync the blockchain **FNL**
- Contact wallet support **FNL**

Segwit (3 addr)

- BCH is incompatible with BTC segwit **FL**

Legacy (1 addr)

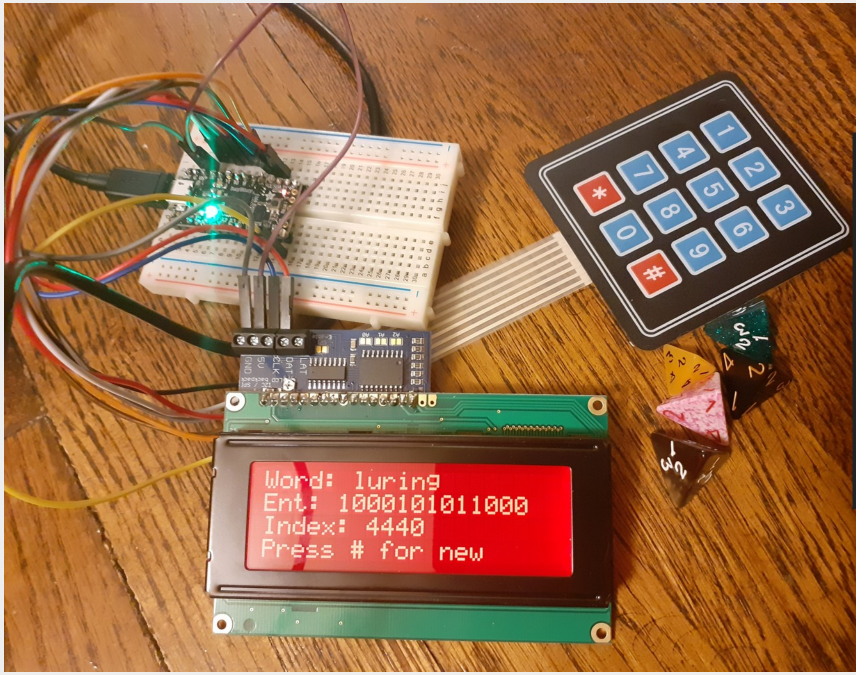
- Follow recovery steps in my tutorials! Probably recoverable **FNL**

FL == Funds lost!
FNL == Funds not lost

User Error #1 - “Cross Chain” Swaps

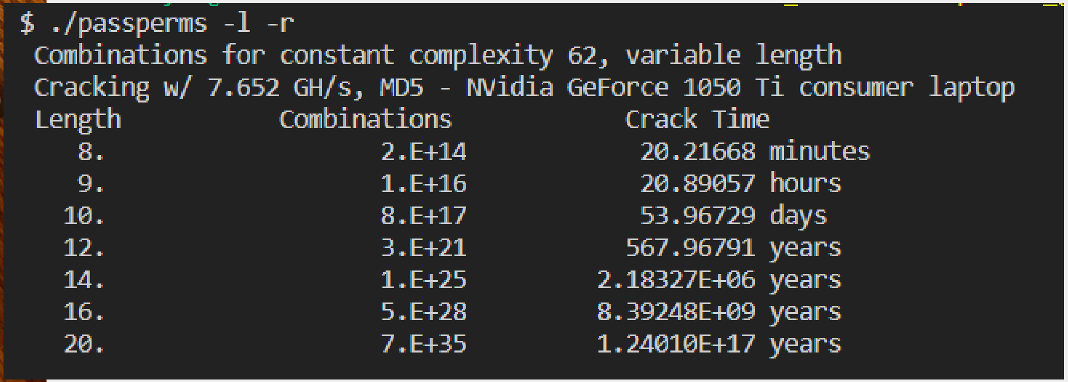
- **Attack:** Not an attack, but a user error.
  - The user mistakenly sends Bitcoin Cash to a Bitcoin address, or mixes one Ethereum token for another.
  - For exchanges, this results in permanent loss of funds. For non-custodial wallets, recovery through manual intervention is *sometimes* possible.
    - I have done successful manual recoveries, but they are 1 in 100
- **Countermeasures:** Always double, triple checking the address belongs to the intended Cryptocurrency
  - **EVERY WALLET UI/UX** should have this warning. None that I know of actually do.

Security Hygiene #1 - Passwords



Entropal – a hardware diceware demo

https://github.com/chaintuts/entropal



```
$ ./passperms -l -r
 Combinations for constant complexity 62, variable length
 Cracking w/ 7.652 GH/s, MD5 - NVidia GeForce 1050 Ti consumer laptop
 Length           Combinations            Crack Time
    8.                    2.E+14            20.21668 minutes
    9.                    1.E+16            20.89057 hours
   10.                    8.E+17            53.96729 days
   12.                    3.E+21           567.96791 years
   14.                    1.E+25         2.18327E+06 years
   16.                    5.E+28         8.39248E+09 years
   20.                    7.E+35         1.24010E+17 years
```

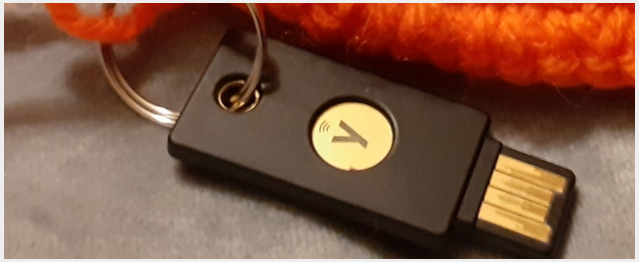
PassPerms – a basic password cracking time demo that shows why length > complexity in general

https://github.com/chaintuts/passperms

Security Hygiene #1 - Passwords

- **Attack:**
  - The user reuses an insecure password between other accounts and an exchanage (ex: Coinbase) or web wallet (ex: blockchain.com).
  - A breach exposes the password and the attacker compromises the user's exchange/wallet accounts
- **Countermeasures:** Proper password hygiene - no password reuse, *long passphrases/randomly generated passphrases,* the use of secure password managers
  - If you own a crypto-related website, *insist* on whatever the industry standard is for user passwords
  - Don’t allow your users to mess this up

Security Hygiene #2 - 2FA



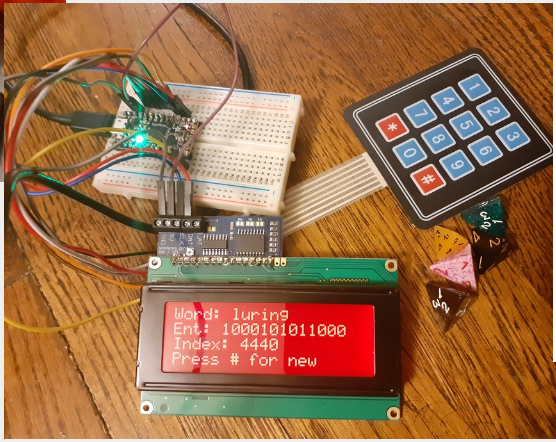
- SIM swaps – an all-too-common plague in the crypto space
- **Attack:**
  - The attacker knows the user has SMS-based 2FA on an exchange and an exposed phone number.
  - The attacker socially engineers the phone company into porting the number to their device.
  - The attacker initiates a password reset to compromise the user's account.
- **Countermeasures:** Only using App-based/TOTP (okay) or security key (best) based 2 factor authentication
  - If you own a crypto related website, *do not* use SMS 2FA. Just don’t.
  - And be the coolest by enabling U2F/FIDO security keys!

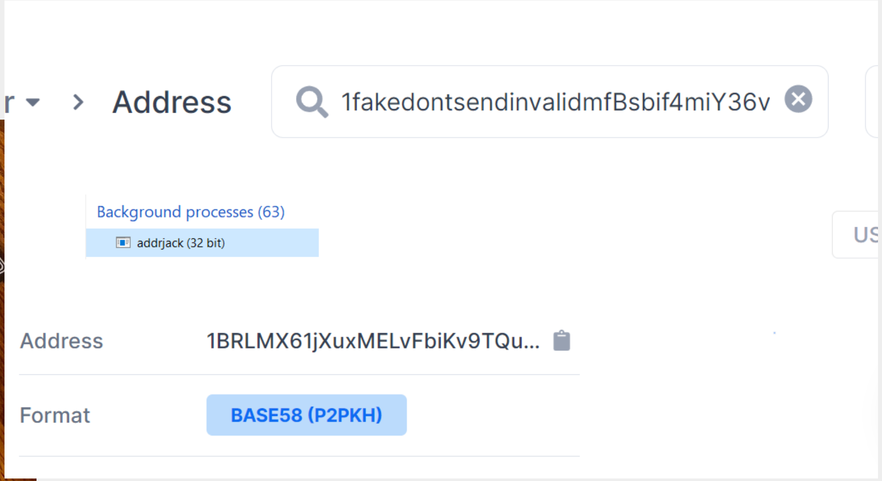
Poor Wallet Implementations

- Wallet implementation/installation issues - ex: Electrum phishing attack, ECDSA nonce reuse, brainwallets
- **Attack:** varies, the attacker uses some poor implementation detail to compromise a wallet software or wallet keys, gaining direct access to user funds
- **Countermeasures:**
  - signature/hash verification of software
  - use of well-audited and reputable wallet software
  - never using brainwallets/paper wallets

Final Thoughts

- A lot of this *probably isn't news to you* – and that's the point
- These are common ways *real people lose money, <u>every day</u>*
- MOST attacks are mitigated by common-sense, relatively non-technical countermeasures
- It's our job as industry professionals to **educate our users, implement sound user experiences, build secure software, and *develop* best practices -** This industry is so new, everyone watching this can be a part of building better security – go do it!





r ▾ › Address 🔍 1fakedontsendinvalidmfBsbif4miY36v ⊗

Background processes (63)

addrjack (32 bit)

US

Address 1BRLMX61jXuxMELvFbiKv9TQu...

Format BASE58 (P2PKH)

Questions?

- Twitter @chaintuts
- chaintuts.com – Contact Form
- DEFCON discord @joshmcintyre#2481

I would love to hear from you – Seriously, get in touch with those questions and feedback!