

OpSec for the Dark Forest

(or how to avoid getting rekt)

Pablo Sabbatella

Web3 Operational Security researcher

OPSEK founder

SEAL 911 contributor



What are we gonna talk about?

Simple things to enhance your Opsec



macOS or Windows? Android or iPhone? Chrome, Safari or Firefox?

It's not the tools you use, but how you use them.

Two factor authentication

Use 2FA (Two factor authentication) on every platform and service you use

- Never with mobile phone number (SMS or call)
- TOTP apps (Authy, Google Authenticator, etc)
 - They are pretty good, but must be configured securely
 - TOTP apps codes can be phished
- Yubikeys are the way to go
 - Yubikeys OTP mode (default) can be phished also. Must be disabled
 - Yubikeys FIDO2 or U2F must be enabled
- You must have two Yubikeys
 - One as the main one, and one for backup.
 - Always configure both in services
 - Nano USB-C and Bio Series USB-C



Section 2

Social Engineering

Everything is an scam until proven otherwise

Be very careful with invitations to calls with

- Recruiters
- VC funds & investors
- Journalists

Don't ever download communication tools others than the one you use: Zoom, Teams, Slack, Discord.

Never install plugins

If something doesn't feel right, it's most probably wrong

- Do not open pdfs from untrusted sources
- Verify who you are talking to, always
- A good con artist will invest time in gaining your trust

Make peace with it

Everyone will eventually get hacked

Yep

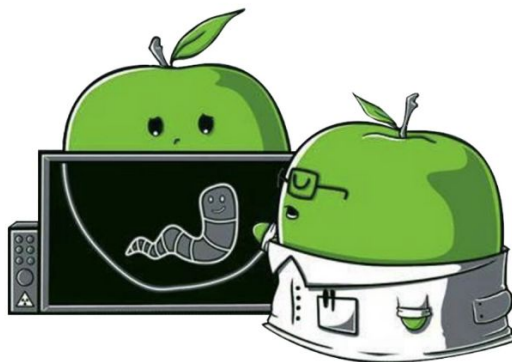
Use an antivirus and firewall



Objective-See
a non-profit 501(c)(3) foundation.



Support Us!



Latest News:

🔧 Tool Update (DNSMonitor):
Just released: **DNSMonitor v1.3.0**

📖 New Blog Post:
Read: **"The Hidden Treasures of Crash Reports"**

🏠 #OBTS v7.0
Just announced **"Objective by the Sea" v7.0**

Featured Tools:



OverSight



KnockKnock



LuLu



BlockBlock



Do Not Disturb

Lulu, Task explorer, BlockBlock, KnockKnock



**The attack will come from a
trusted source**

From: "ether.fi" <noreply@event.eventbrite.com>

Date: May 29, 2024 at 1:02:20 PM EDT

To: [REDACTED]

Subject: Event update: Your Pass to the ether.fi's DeFi Event at Consensus!

Reply-To: etherfievents@outlook.com



This was sent to you by [ether.fi](#)

Hey,

Just a quick heads up that [ether.fi](#)'s DeFi Event at Consensus is almost upon us! Due to the overwhelming response, we would like to inform you that you need to mint your NFT pass to gain access to the event.

Mint your NFT pass - [LINK](#)

Your NFT pass will allow you to attend the upcoming event on May 29 at: [Estelle's](#)

Not only will your NFT pass grant you access to the main event, but it'll also grant you a secret bonus.

Since space is limited, we suggest you secure your spot by minting your NFT pass today! If you have any questions, feel free to get in touch.

See you at the [ether.fi](#)'s DeFi Event at Consensus!

Best regards,
[ether.fi](#)

Assets undergoing upgrade

Inbox x



Trezor <noreply@trezor.io>

[Unsubscribe](#)

to me ▾

11:37 AM (0 minutes ago)



Reply



Dear customer.

This email is to let you know your wallet assets are undergoing a upgrade.

In an effort to upgrade our infrastructure we are temporarily disabling the following networks:

BTC, ETH, XRP, ERC20, BEP20, TRON, TRC20

We are requiring action from our users to re-enable the networks.

Important: Failure to upgrade your networks could result to full funds loss.

suite.trezor.io/upgrade

Copyright © 2022 TREZOR LABS.
a part of SatoshiLabs Group.

If you wish to unsubscribe from our newsletter, click [here](#)

← Reply

→ Forward







Trezor <noreply@trezor.io>

[Unsubscribe](#)

to me ▾

from: **Trezor** <noreply@trezor.io>
reply-to: noreply@trezor.io
to:
date: Jan 24, 2024, 11:37 AM
subject: Assets undergoing upgrade
mailing list: NDc5NDcONC0xMjlyNTktMTE=
<NDc5NDcONC0xMjlyNTktMTE=.list-id.mailing.trezor.io> [Filter](#)
[messages from this mailing list](#)
mailed-by: mailing.trezor.io
signed-by: trezor.io
unsubscribe: [Unsubscribe from this mailing list](#)
security:  Standard encryption (TLS) [Learn more](#)
 Important according to Google magic.

[sure.trezor.io/upgrade](#)

Never reuse them

Use a password manager

Yep

But never put seed phrases on them

Hot wallets are are for small stuff

Use hardware wallets



**85% of lost funds are
due to poor
operational security**

Thank you!

Pablo Sabbatella

Opsek founder, SEAL member.

@pablosabbatella

