An Ultimate List of Rules Net Survivors Should Follow to Stay Safe!

Operational security professionals work to figure out where their information can be breached. That said, it doesn't really matter what industry you're in. If you have any sensitive, proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind!

Disclaimer ❗ All of the information on my blog and on my social media sites, including this article, is strictly for introductory purposes!

Looking at operations from a malicious third-party's perspective allows us to spot vulnerabilities we may have otherwise missed so that we can implement proper countermeasures…

The most important thing to understand here is the path of the cyber attack – its vector. Let's take a closer look at various problems associated with OpSec and its implementation to modern life!

I - Basic Security Knowledge

Email

Use a secure email provider like Protonmail or Tutanota. Also, use a trusted VPN like Mullvad or ProtonVPN. E2E (end-to-end) encryption is only as secure as the service you are sending the email to.

For example, if a Protonmail user sends an email to a GMail user, the email is encrypted with TLS, but Google can still read and hand over any data that passes through their server. E2E can be re-established by using features such as the password-protected email feature from Protonmail.

Password

Use different emails and different strong passwords. Store them in one place like a password manager. Never reuse passwords, especially for accounts with personally identifiable and sensitive information (e.g. Facebook, Gmail, AppleID, Twitter, banks/payments, crypto accounts).

Use passwords that are at least 8 characters in length, but a minimum of 12 is generally recommended for memorization. Along with that, if using memorization, ensure that a minimum complexity requirement is met: which means having an uppercase character, a lowercase character, a digit, and a non-alphabetic character.

Using a string of unrelated words while still meeting the dictionary requirement makes it easy to have an extremely secure password while still being able to remember it. If fully relying on a password manager, a password of 20+ characters in length that is randomly generated can be used.

If you see suspicious password activity or failed log-ins on any of your accounts, change all of your passwords, starting with sensitive and authorization accounts, such as your primary email and bank/crypto accounts. Keepass or BitWarden are good options.

Phone

Never link phone numbers to crypto platforms. Use trusted multiple e-sims if you have to link the phone. To lock down your SIM, contact your mobile phone carrier. Ask them to NEVER make changes to your phone number/SIM unless you physically show up to a specific store with at minimum two forms of identification.

This (should) prevent hackers from calling up AT&T or T-Mobile or Vodafone, claiming to be you, and asking them to port your phone number to a new phone.

OTP & 2FA

Instead of SMS-based 2FA, use Aegis OTP for iOS or Android. Google Authenticator is generally not recommended anymore in order to stay out of the Google ecosystem, and Authy offers more robust account recovery options (Aegis does not offer the same level of account recovery options).

Keep in mind that the codes generated by 2FA apps are device-specific. If your account is not manually backed up to Google cloud or iCloud and you lose your phone, you'll need to spend some time proving your identity to restore your 2FA.

The added security is worth the hassle!

Hardware-based 2FA options are regarded as more secure than phone-based OTP options since the keys are stored on the YubiKey device itself, not on your phone, or in the cloud, or on your computer.

Cold Storage

Cold storage, and separate “hot” wallet. Use multisig (gnosis-safe as example) or at least a hardware wallet. Never store your seed phrase digitally.

Seed phrases are intended to be stored on the paper card included with hardware wallets! That means never type it up, store it online, or take a photo of the card.

Store your key on hard device. Separate devices to which you are connecting your cold storage. By separating crypto, work, and leisure you greatly increase your productivity and focus.

Back-ups

Offline back-ups. Store them in a safe. Can be written on paper, but recommended to be etched or laser-printed into metal. Always be sure to have a backup stored somewhere safe if your threat model allows for that.

Ask yourself, what happens if my house catches on fire? What temperature is my safe rated to? Some individuals find a safety deposit box handy.

Anti-Virus

Never do anything you do not understand. Always check which token you approve, the transaction you sign, assets you send, etc - be extremely accurate while making any financial operation.

Keep in mind that one of possible attack vectors is to put you in a situation that will encourage you to do something (login or anything like that).

You can install malwarebytes or Comodo or DrWeb antivirus but it won't help you if you do not understand them. Keep up your basic set of defending tools up to date.

Address

Be careful about using your real home address online for delivery purposes. Data breaches are now a daily occurrence, and many breaches include customer names and addresses.

Your physical address is not as easily changeable as a phone number or email address, so be especially mindful about where you use it on the Internet.

If you’re ordering pizza with crypto, order it for pickup instead of delivery.

When online shopping, use a different (and publicly available) address for package delivery. Options here include your workplace or drop boxes at delivery service providers like FedEx and your local postal service.

An important tip

Remember: You Could Be a Target! We are a natural target for all sorts of attacks — from garden-variety cybercriminals to competitive spying (sounds dramatic, but it’s real!).

That said, it doesn’t really matter what industry you’re in. If you have any sensitive, proprietary information at all (and let’s face it, most people in crypto do), then you could very well be a target. This is a good thing to always keep in mind.

A culture of skepticism

Remain Vigilant - Create a culture of skepticism where they feel comfortable checking twice before clicking a link or responding to a request for sensitive information, and you’ll have a much more secure organization overall.

Analyze security holes and other vulnerabilities. Assess your current safeguards and determine what, if any, loopholes or weaknesses exist that may be exploited to gain access to your sensitive data.

OpSec in public

OpSec often comes into play in public settings. For example, if members of your team are discussing work-related matters at a nearby lunch spot, during a conference, or over a beer, odds are that someone could overhear.

As they say, loose lips can sink ships, so make sure you don’t discuss any sensitive company information while out in public.

Many OpSec missteps can be avoided by being more aware of your surroundings and the context in which you are speaking: what you're saying, where you are, who you're speaking to, and who might overhear.

It's a good idea to go over the "no-no's" for your specific company during onboarding and to remind employees of them periodically.

Separating data

Identify your sensitive data, including your product research, intellectual property, financial statements, customer information, and employee information. This will be the data you will need to focus your resources on protecting.

Security awareness

Identify possible threats. For each category of information that you deem sensitive, you should identify what kinds of threats are present.

While you should be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers. Implement separation of duties. Make sure that those who work on your network are not the same people in charge of security.

Estimate losses

Appraise the level of risk associated with each vulnerability. Rank your vulnerabilities using factors such as the likelihood of an attack happening, the extent of damage that you would suffer, and the amount of work and time you would need to recover.

The more likely and damaging an attack is, the more you should prioritize mitigating the associated risk.

Countermeasures

Get countermeasures in place. The last step of operational security is to create and implement a plan to eliminate threats and mitigate risks. This could include updating your hardware, creating new policies regarding sensitive data, or training employees on sound security practices and company policies.

Countermeasures should be straightforward and simple. Employees should be able to implement the measures required on their part with or without additional training. Incident response and disaster recovery planning are as well crucial components of a sound security posture.

Even when operational security measures are robust, you must have a plan to identify risks, respond to them, and mitigate potential damages.

Keep your enemies close

Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is. But I'd say it sounds pretty okay.

II - OpSec when holding or working in Crypto industry

Starting up...

Understand that all sorts of blockchain.info, TrustWallet, MetaMask and other wallets are just interfaces. Make a cold wallet yourself. For example, from an old smartphone. You can also make a cold wallet with Electrum and let all the traffic through Tor.

Know AirGap weak sides.

Never use your main cold storage and «Back Office PC» for casual work, but if you have to do it (and you know why you are doing it), use only open-source wallets!

Check out what are you signing and to which contract you are giving an approve!

Check what are you signing, if we speak about ETH and similar chains, never use your main cold storage for casual work, but if you have to (for example, sign a gnosis-safe multi-sig (2) (3) transaction), always check if there are no allowance approve(which allows to drain your wallet) or proxy (behind which mentioned function may be hiding).

Revoke approvals here.

Be extremely aware when using a clipboard!

Always double-check an address you've copied to the clipboard. There is an evil software existing which is called a Clipper - it can replace an address in your clipboard to a very similar-looking hacker's address which has the same symbols in the beginning and in the end as your original address.

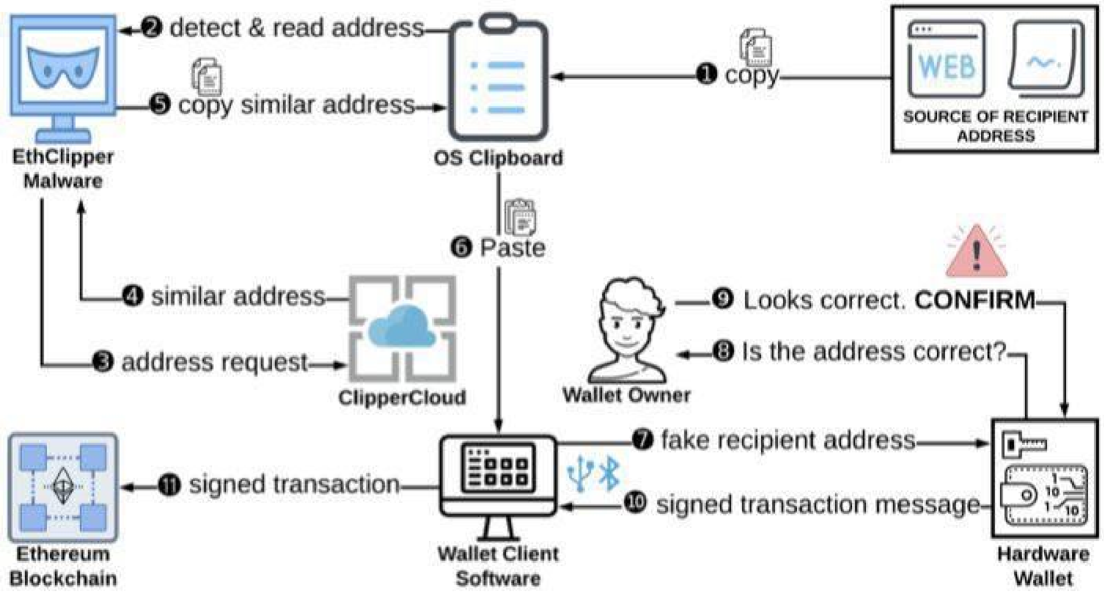

Fig. 4: **Workflow of the *EthClipper* attack.** ❶: The owner of the wallet copies a recipient address to the clipboard from the source (e.g., website); ❷: the *EthClipper* malware detects the address in the clipboard; ❸: the malware connects to *ClipperCloud* to request an address that is similar to the one in the clipboard; ❹: *ClipperCloud* replies with a similar address; ❺: *EthClipper* malware places the substitute address from *ClipperCloud* to the clipboard; ❻: the user of the wallet pastes the address from the clipboard to the hardware wallet's client software; ❼: the client software sends the transaction data, which includes the replaced (fake) recipient address, to the hardware wallet for signing; ❽: the hardware wallet asks the user to confirm the parameters of the transaction (by pushing a button on the wallet); ❾: the user of the hardware wallet, who is prone to a confirmation bias, confirms the transaction without verifying all of the symbols of the recipient address; ❿: the wallet signs the transaction using the air-gapped private key and sends the signature to the wallet's client software; ⓫: finally, the wallet client software sends the signed transaction to the Ethereum blockchain, where the transaction is executed.

Physical Attacks be like...

Accept as a fact that if the device falls into the hands of intruders, only custom capacitors can save your money (so that you can not get directly to the brains and read electric signals) and other things like self-destruction, epoxy, and so on.

That is, ideally, you can not allow physical contact in any case. You can use special logic bombs or logic gates, extra passwords that trigger some kind of security action, alert events on your address via tenderly.co or Forta or using 2/3 multi-sig all the time from 3 different devices.

Anyway remember, the device must not fall into anyone's hands.

One could also create a honeypot wallet and have a script that listens for tx's originating from those addresses that alerts authorities, security companies and/or friends & family that you are under duress, perhaps even sending your location or last known location based off a GPS chip phone with the alerts.

Forewarned is forearmed

Be aware of modern attack methods, carefully read step-by-step my Guide and a Compendium, you don't need a deep understanding of how hacks work exactly but that's important to know how does it looks like to be a victim. Counter-OSINT is important here as well.

Read about it more here and here.

Study threat modeling (2) (3) and establish all possible threats even if they seem crazy to you. Being suspicion is always a good thing.

After all, fake news only works best with those who carry it to their acquaintances, becoming a kind of donor.

In the same way with attacks, very often you may try to be hacked through acquaintances, pretending to be acquaintances or acquaintances themselves.

> Always keep this in mind. This world is cruel and dangerous.

III - Crypto OpSec on steroids

If we finally want to give people the opportunity to be their own bank, we must realize that in this case people must be able to replace all those services and actions for which traditional banks get money.

Banks have long been concerned about creating a system of protection not only in meeting rooms and the office management, but also in the security departments. Banks can use deep underground laboratories and huge Faraday cages for this purpose.

I am not asking you to comply with all of this, but you must remember the main rule:

> *Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.*

Awesome security guides to follow:

Anonymity:

• hackmd.io/YKjhguQES_KeKYs-v1YC1w?both

• DeepWeb/DarkNet OpSec Guide 2022

Privacy:

• yawnbox.com/blog/how-to-use-an-ipad-as-a-secure-calling-and-messaging-device

• privacyguides.org

OpSec:

• www.usenix.org/system/files/1401_08-12_mickens.pdf

For deals use escrow and tx alarm clock and with special services like safient.io, sarcophagus.io, safehaven.io. Use OpenSource password storage, s__elf-hosted link system__, reliable communication method from this sheet, use OpSec services, be aware of the latest anonymity and privacy techniques.

Carefully read step-by-step my guide once again.

Don’t be afraid of links, you don’t need **all** of **them** but you should be able to pick up which will interest you the most for your own Pathway. Use extensive measures when working with files and always keep an eye on the latest security trends even if your area is far from it.

Take this subreddit and this awesome old & trusted resource as the first step.In our dangerous world anyone can become a target, especially in crypto.

It sounds scary but it is possible, the main thing is to always think ahead.

Check out my OpSec Guide:

- Portuguese-Brazilian
- Russian

- French
- English

Kogaan! Zu'u wah dein hin faraan! 🐉

If you want to support my work, please consider donating me:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A** or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU** - BTC
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

Stay Safe!