

# Personal SecOps for your ...

... corporate persona + Privacy is past tense  
«personal cybersecurity» series

*author: Timur 'x' Khrotko*  
*R2411.h*



# whoami

Timur 'x' Khrotko


- [x@def.dev](mailto:x@def.dev) – dev sec trainings / audits
- [timur@owasp.org](mailto:timur@owasp.org)
- [linkedin.com/in/timurx](https://www.linkedin.com/in/timurx)
- [github: timurxyz](https://github.com/timurxyz)
- phd

*> and you?*



Paraniod mindset brought me here

**RULE#1: Relax, don't be paranoid ,)**

*Your being secure  
shouldn't feel like* 

***Who/what is your antagonist***

I'm an average Mary/Joe/They

VS

I'm Mr/Mme Target

# *Spectrum of security/safety*

Stealth mode \*



....



Easy target

\* impossible

# Practical threat model

- Feasible risks
  - realistic ones + surprises
    - support scam, deep fake, voice spoofing, fake landing pages
  - risk = **loss \* likelihood ~ bias**
- Tell yourself scary stories
  - dream up your antagonists
    - skills, routines, professionalism
    - motivation, organization/organizedness
    - resources, budgets
  - corporate approach
    - valuable assets
    - cyber-enabled capabilities
    - vulnerable surfaces
    - negative technical impact...

## In a nutshell

**Tune** the below aspects of your personal cybersecurity in accordance with **your own risks** and circumstances

- Your digital identities / **personas**
  - multiple, structured
- Your **devices**
  - updating, multiple, trusted and roadwarrior ones + nihilist
- The **tools** you use
  - updated, structured, reliable, interoperable
- The **how**
  - conscious, routine, non-paranoid + nihilist
- Secrets
  - **keys**, passwords, passwordless, MFA, biometrics



# Guidelines

- Electronic Frontier Foundation, Surveillance Self-Defense



- <https://ssd.eff.org/>

- BSI Minimum standard [DE]

- [https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards\\_node.html](https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html)

- NSA Cybersecurity Advisories & Guidance

- <https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/>



# Threat trends / '23 / IBM X-Force

## THREATS

- ✓ IDENTITY
- ✓ DATA
- ✓ APPS
- ✓ GENAI

- 2023 →
- 800K
- ALT



stay tuned.

## OWASP

MISCONF	30%	} 36% IAM
ID/AUTHN	21%	
ACC CTRL	15%	

## GOOD NEWS

- 0 DAYS ↓ 72%
- RANSOMWARE ↓ 12%

# Threat trends / '23 / IBM X-Force

## THREATS

- ☑ IDENTITY
- ☑ DATA
- ☑ APPS
- ☑ GENAI



you'll be following these industry best practices

## RECOMMENDATIONS

- MFA, PASSKEY
- ENCRYPT, B/U
- PATCH, HARDEN
- LEARN

84% → BP



Hackers don't  
break in.

**They log in.**



password

password+  
Conditional MFA

multi-device  
"passkey"

Device-bound  
FIDO credential

Passizé #phishproof

# INTERLUDE

*Privacy is past tense*





**Craig Balding** · 1st

Independent Cyber Security Consultant

1w · Edited ·



## ChatGPT AVM Stole My Voice

This morning my helpful assistant ChatGPT spoke back to me in my own voice during our walk and talk.

Not a similar voice - my voice. Enough to make me stop in my tracks.

And this wasn't a one-off incident.

OpenAI's recent system card revealed their GPT-4o model unexpectedly cloned and used a Red Team tester's voice mid-conversation. They don't call it cloning, rather "Unauthorized voice generation" (maybe someone at OpenAI was watching too many "Yes, Minister" YouTube clips)

Here's the trippy 42-second clip that made the Red Teamer sit up straight:

# Chat Control 2.0

The **Regulation to Prevent and Combat Child Sexual Abuse (Child Sexual Abuse Regulation, or CSAR)** is a [European Union regulation](#) proposed by the [European Commissioner for Home Affairs Ylva Johansson](#) on 11 May 2022. The stated aim of the legislation is to prevent child sexual abuse online through the implementation of a number of measures, including the establishment of a framework that would make the detection and reporting of child sexual abuse material ([CSAM](#)) by digital platforms – known by its critics as **Chat Control** – a legal requirement within the European Union.<sup>[1][2]</sup>

## Background [\[ edit \]](#)

---

The [ePrivacy Directive](#) is an [EU directive](#) concerning digital privacy. In 2021, the EU passed a temporary [derogation](#) to it – called Chat Control 1.0 by critics – which allowed email and communication providers to search messages for presence of CSAM.<sup>[3][4]</sup> It was not mandatory and did not affect [end-to-end encrypted](#) messages. The purpose of CSAR – called Chat Control 2.0 by critics – is to make it mandatory for service providers to scan messages for CSAM, and to bypass end-to-end encryption.<sup>[3]</sup>



# Palantir Gotham

“ The functionality in Palantir's Europa release has changed how my organisation fights crime. In addition to protecting data better, we are able to incorporate digital forensics into our workflows in ways that we could only imagine just a few years ago.

↳ European Law Enforcement Official



Investigators can map out key pieces of evidence associated with an entity of interest, such as phone records associated with a

Analysts can explore relationships between

# Palantir El Salvador

"e- monitoring of public space"



"e- investigator and judge"



2. **Transparency and Accountability:** There have been concerns about the lack of transparency and accountability in Palantir's operations in El Salvador, including the limited availability of information about the company's contracts and activities.

## Conclusion

Palantir El Salvador plays a significant role in supporting the government and private sector in El Salvador, leveraging data integration and analytics to drive positive change. While challenges and controversies exist, Palantir's presence has the potential to contribute to improved governance, security, and economic development in the region.

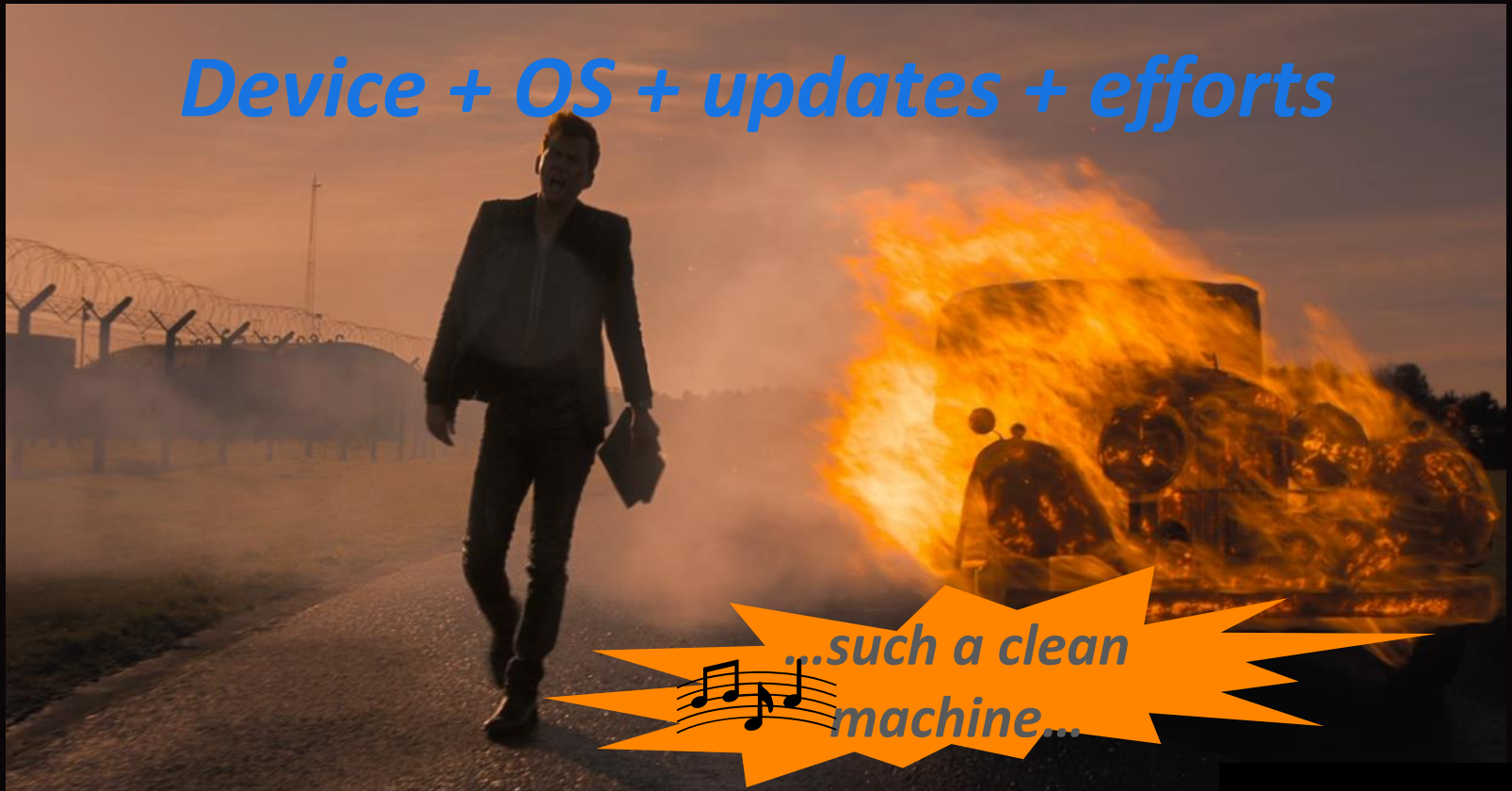




Fizetés mosollyal / Sberbank

## **RULE#2: Have a trusted machine**

*Device + OS + updates + efforts*



*...such a clean  
machine...*





\* Yubikey

# Android = Google Pixel

Nouveau

## Pixel 9 Pro Fold avec Gemini

L'IA de Google, en mode spectaculaire.

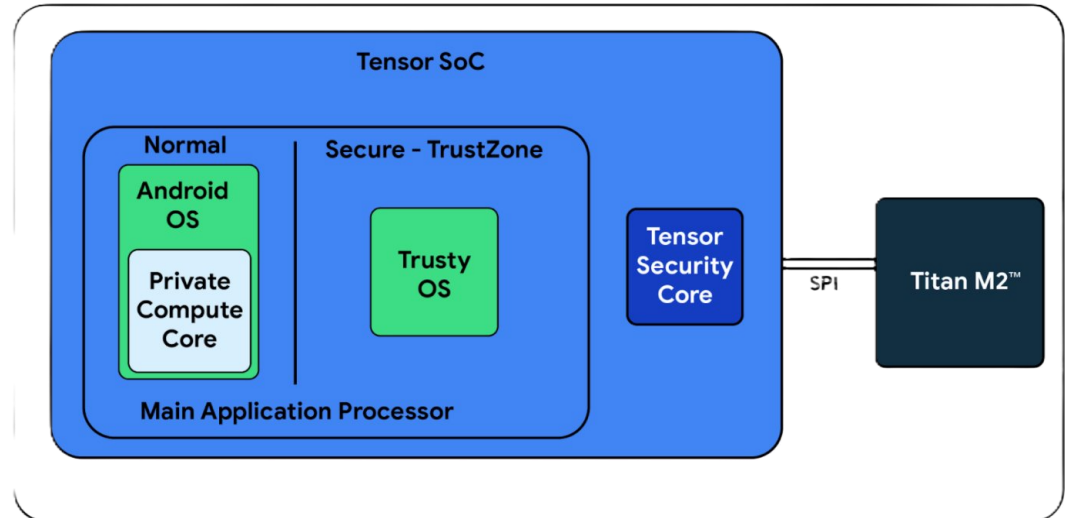
À partir de 1799 € ~~1899 €~~ Économisez 100 €

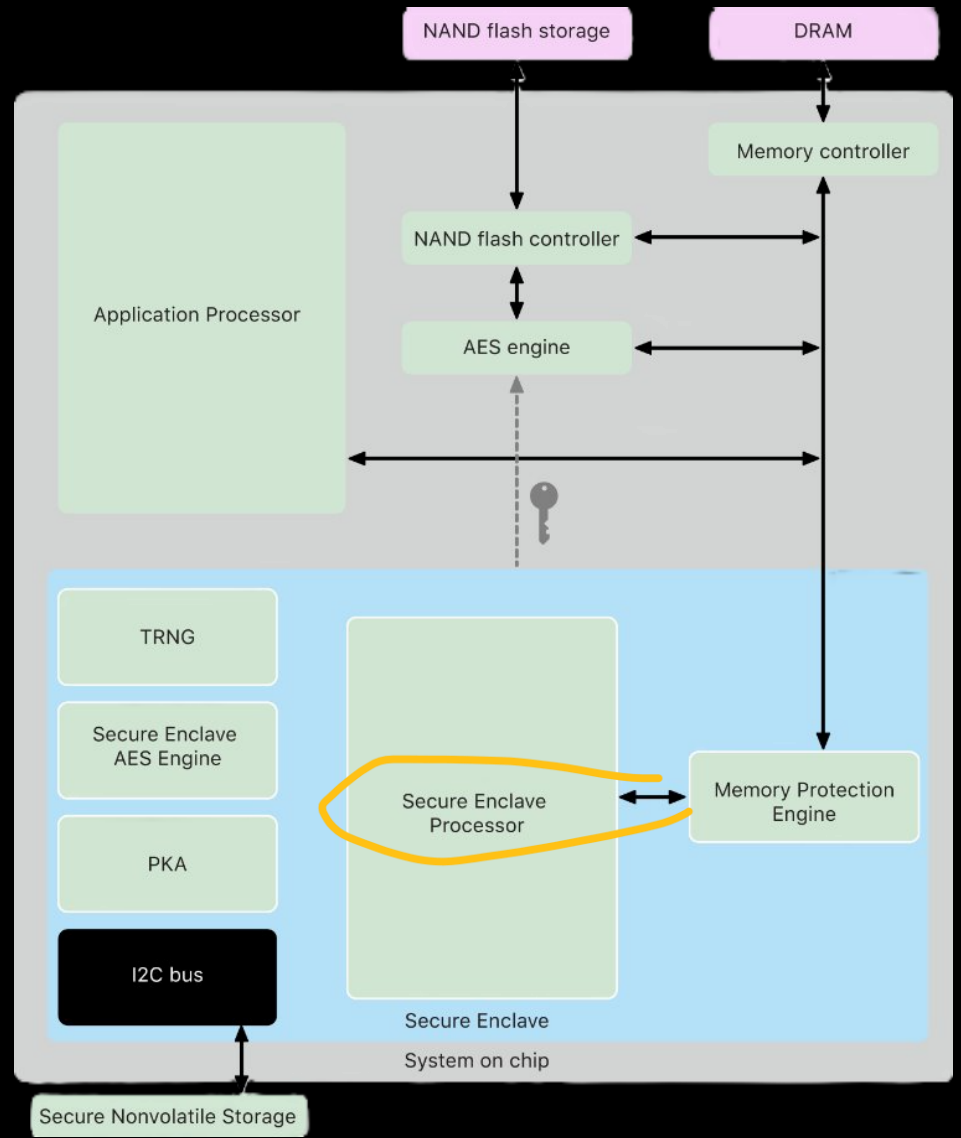
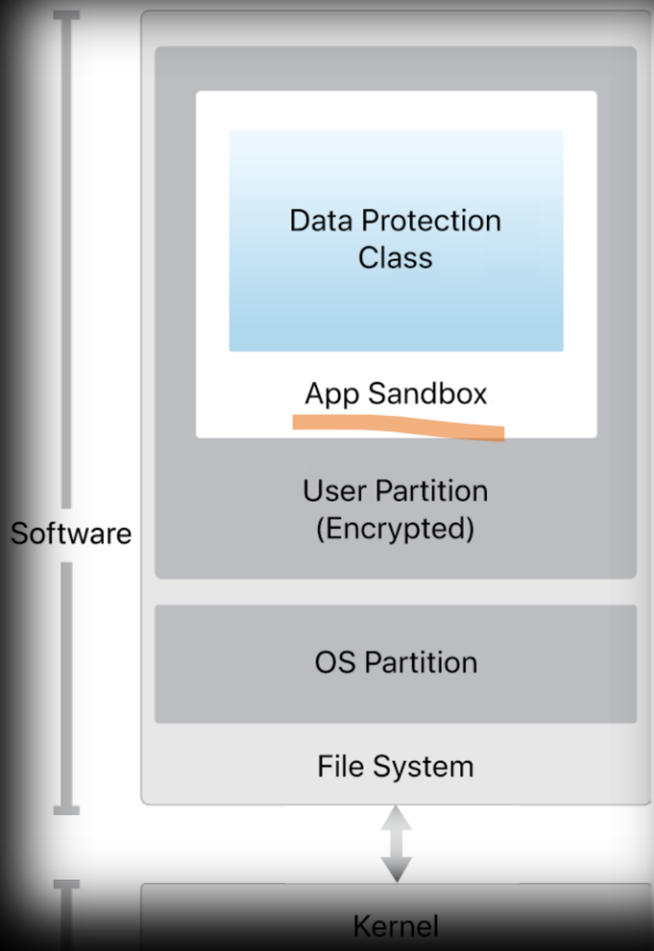
ou 599,67 €/mois en 3 mensualités\*

Prix de vente habituel : 1899 €

[En savoir plus](#)


[Acheter >](#)





A secure by design platform: **iOS/iPhone**

SECURITY

 Stolen Device Protection  
On >

 Lockdown Mode On >

0:45

5G 47

 **Privacy & Security**  
Sensitive Content  
Warning Off >

Detect nude photos and videos before they are viewed on your iPhone, and receive guidance to help make a safe choice. Apple does not have access to the photos or videos. Learn more...


 Analytics & Improvements >

 Apple Advertising >

TRANSPARENCY LOGS

 App Privacy Report Off >

SECURITY

 Stolen Device Protection  
On >

 Lockdown Mode On >



[Back](#) Lockdown Mode

## Lockdown Mode

Turn on this extreme protection if you believe you're being targeted in a cyberattack. Apps, websites and feature functionality will be limited, and some experiences may be completely unavailable.

[Learn more...](#)[Turn Off Lockdown Mode](#)

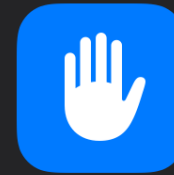
### Messages

Most message attachments are blocked and some features are unavailable.

### FaceTime

Incoming FaceTime calls from people you have not previously called are blocked. Features such as SharePlay and Live Photos are unavailable.

'23 &gt;

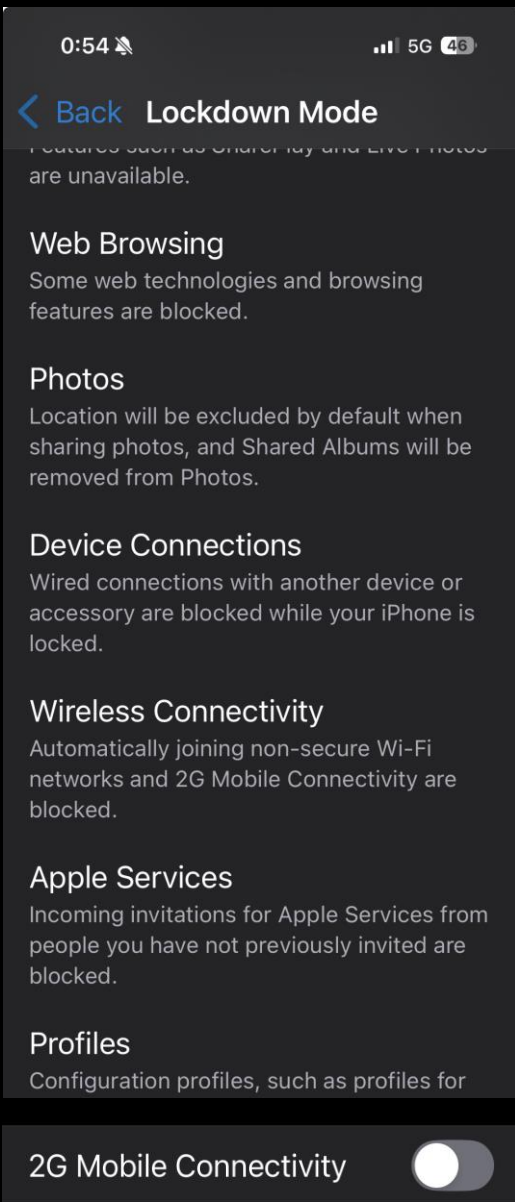


## Lockdown Mode

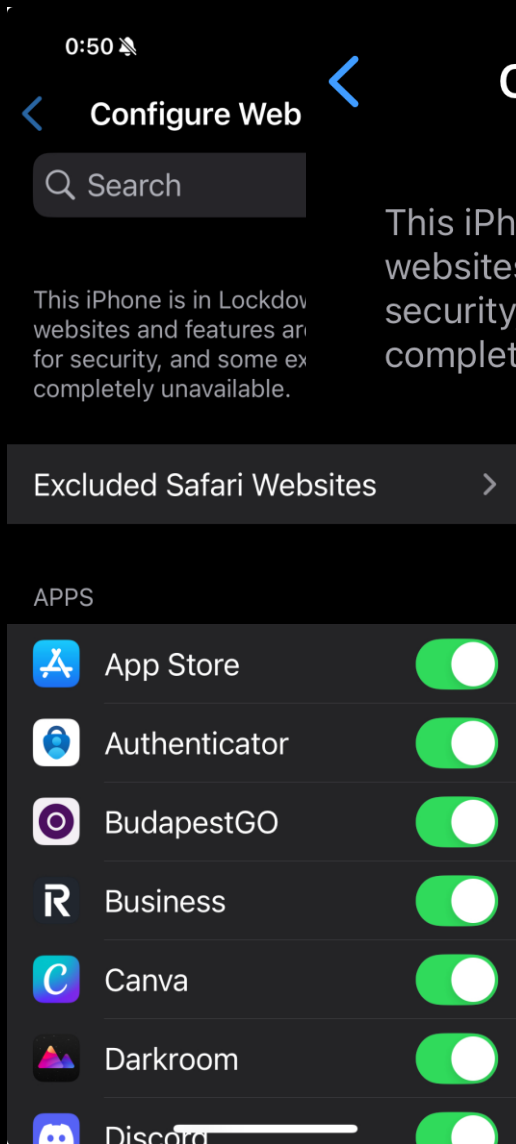
Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

For complete protection, Lockdown Mode has to be enabled on all your devices. Apps, websites and features will be strictly limited for security, and some experiences will be completely unavailable.

[Learn more...](#)

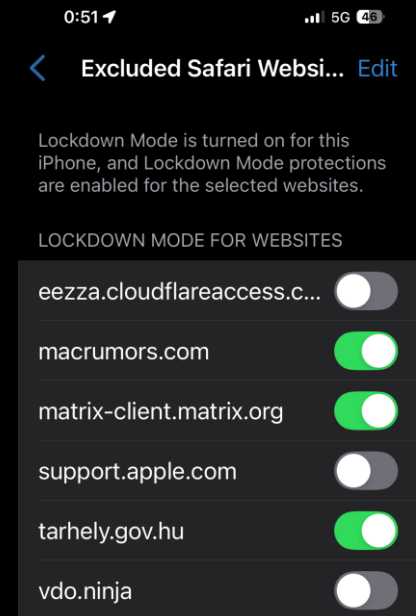


For enhanced security, 2G mobile connectivity is turned off when in Lockdown Mode. Emergency calls may temporarily turn on 2G, if needed.



## Configure Web Browsing

This iPhone is in Lockdown Mode. Apps, websites and features are strictly limited for security, and some experiences are completely unavailable.



Navigation icons: back, forward, search, share, play

practical-private.D0.Fastforward.1910.tx.\_wip\_f

Home Insert Draw Design Transitions Animations Slide Show Review

New Slide Layout B I U A A

## In a nutshell

Tune the below aspects of your personal cybersecurity in accordance with your own risks and circumstances

- Your digital identities
  - multiple, structured
- Your devices
  - multiple, trusted and roadwarrior ones
- The tools you use
  - structured, reliable
- The how
  - conscious, routine, non-paranoid
- Secrets
  - keys, passwords, bio

All rights reserved def[dev]eu

Slide 6 of 36

Navigation bar with slide thumbnails and dock icons (Messages, Safari, Files, App Store, Music, Photos, PowerPoint, Drive)

< Browse Edit ...

```

apt-get upgrade
apt-get update
shutdown -r now

nano -w /etc/ssh/sshd_config
?

pwd quality?

timedatectl set-timezone
Europe/Berlin
date

apt-get install unzip

https://github.com/trailofbits/
algo
3

mkdir /opt/; cd /opt
wget
https://github.com/trailofbits/
algo/archive/master.zip
unzip master.zip

cd algo-master

https://github.com/trailofbits/

```

nano config.cfg

# Chromebook

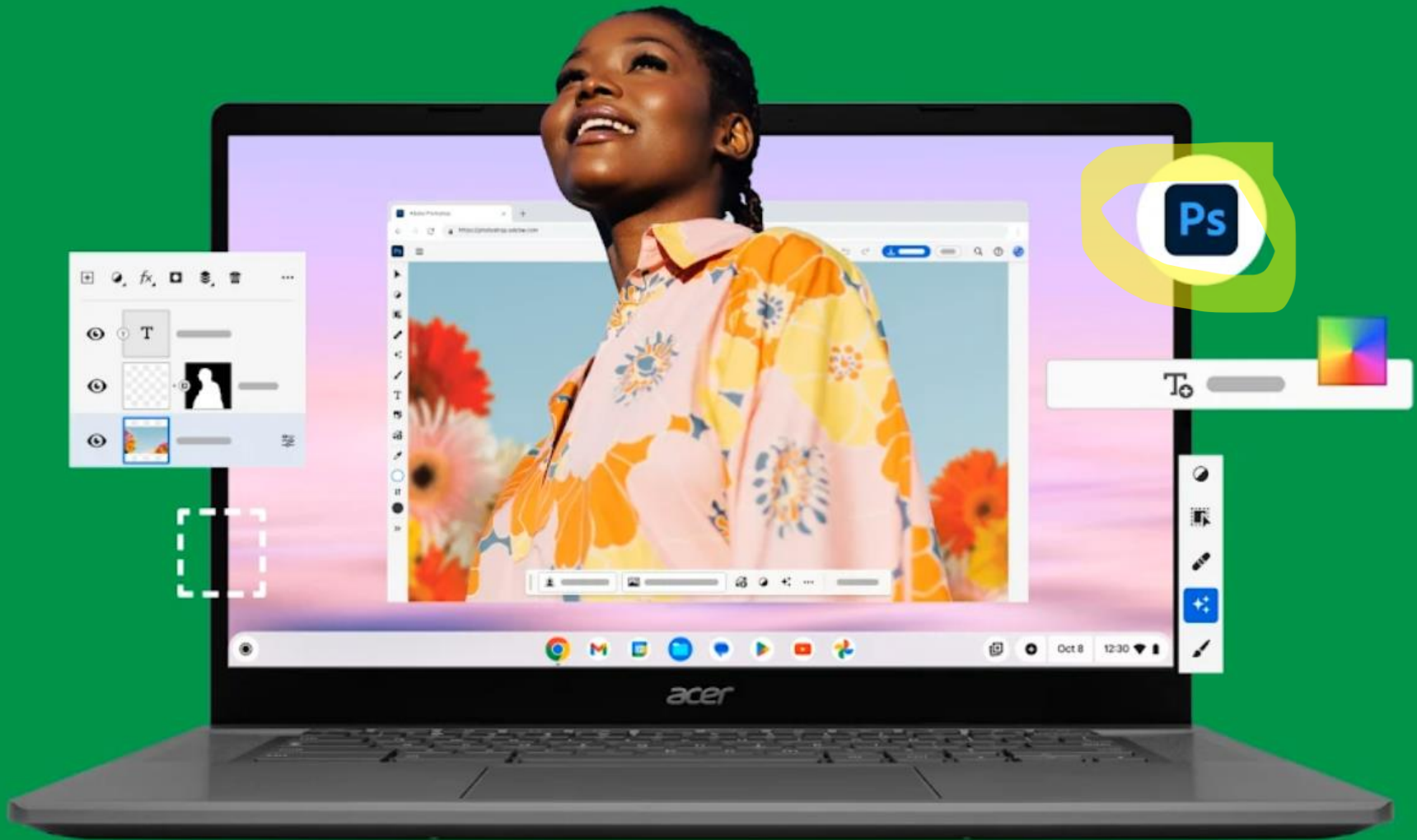
FAST BOOT



INTERRUPTION-FREE UPDATES



You don't need Windows/Mac apps!



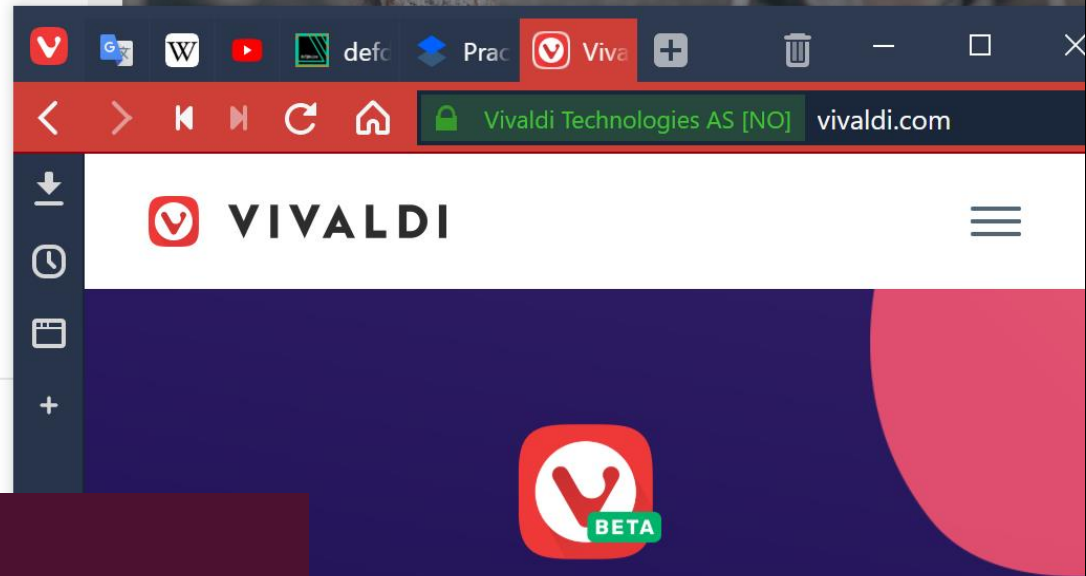
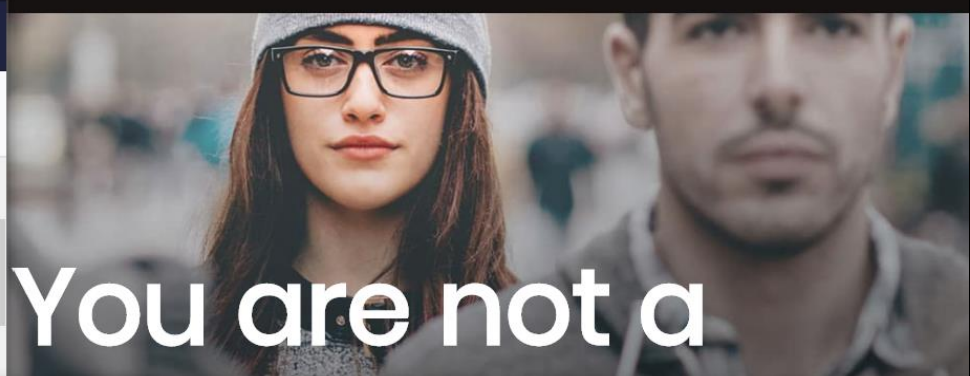
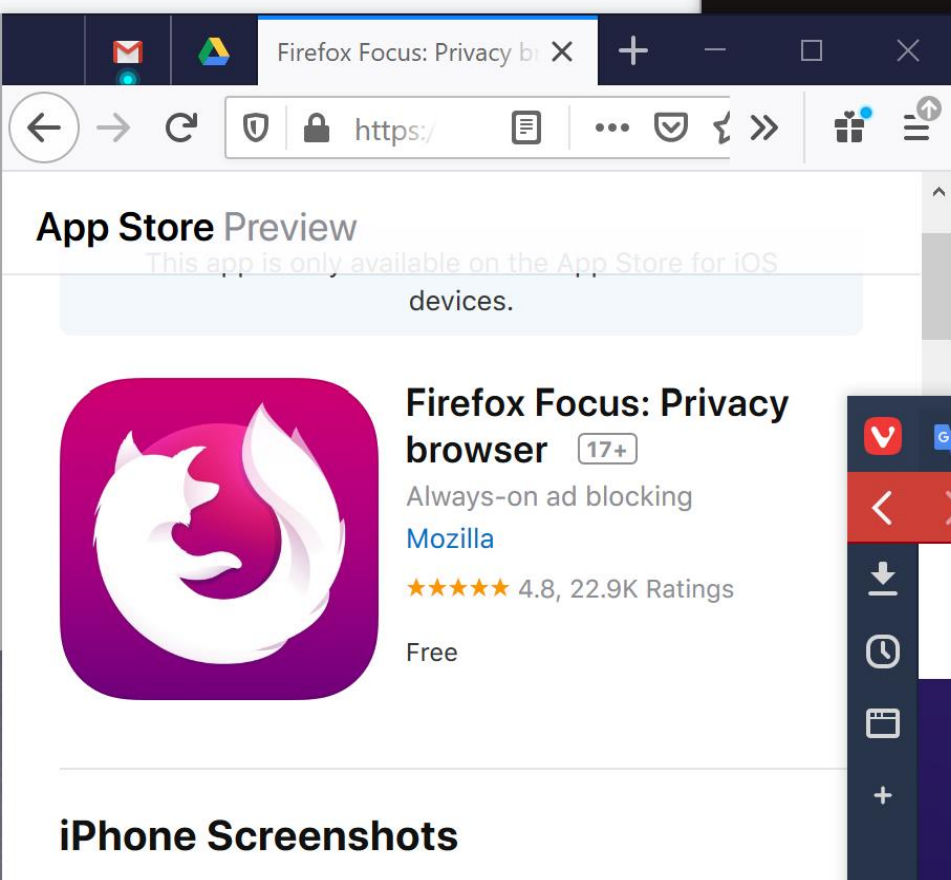
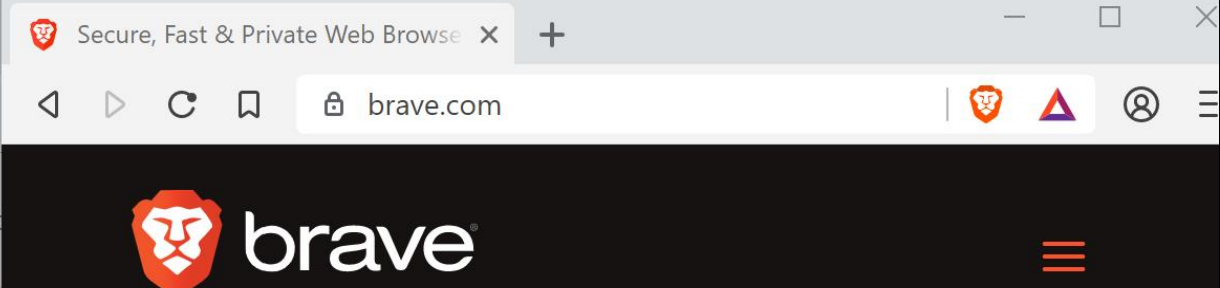
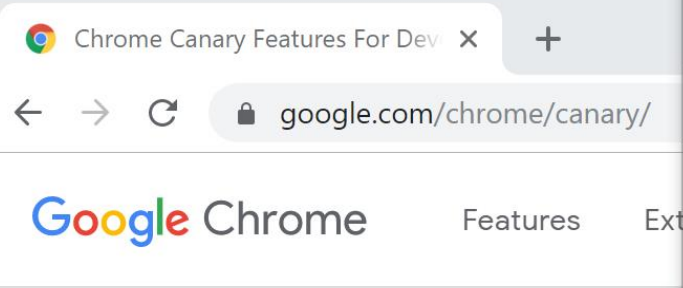
## **RULE#3: Browser polygamy**

*Min 1 browser / 1 persona*

# Multirole of you: your digital Shiva







**Browser polygamy**

**Vivaldi Android Beta**





**RULE#4: Trust Chrome browser**

*Help it to help you*



# Settings

Search settings

- You and Google
- Autofill and passwords
- Privacy and security**
- Performance
- Appearance
- Search engine
- Default browser
- On start-up
- Languages
- Downloads
- Accessibility
- System
- Reset settings

## Security

### Safe Browsing

#### Enhanced protection

- Real-time, AI-powered protection against dangerous sites, downloads and extensions that's based on your browsing data getting sent to Google

#### When on

- Warns you about dangerous sites, even ones that Google didn't know about before, by analysing more data from sites than standard protection. You can choose to skip Chrome warnings.
- In-depth scans for suspicious downloads.
- When you're signed in, protects you across Google services.
- Improves security for you and everyone on the web.
- Warns you if you use a password that has been compromised in a data breach.

#### Things to consider

- Sends the URLs of sites you visit and a small sample of page content, downloads, extension activity and system information to **Google Safe Browsing** to check if they're harmful.
- When you're signed in, this data is linked to your Google Account to protect you across Google services, for example increased protection in Gmail after a security incident.
- Doesn't noticeably slow down your browser or device.

Learn more about [how Chrome keeps your data safe](#)

**A good safety / privacy tradeoff**

are known to be dangerous. When



newyorktmes.com

- All
- Videos
- Images
- Maps
- News
- More
- Settings
- Tools

About 4,470,000 results (0.52 seconds)

Did you mean: [newyorktimes.com](#)

[newyorktmes.com/](#)

No information is available for this page.  
Learn why

[NewYorkTimes.com](#)

<https://newyorktimes.com>

No information is available for this page.  
Learn why

[The New York Times - Breaking News, World News ...](#)

<https://www.nytimes.com>

The New York Times: Find breaking news, multimedia, reviews & opinion on Washington, business, sports, movies, travel, books, jobs, education, real estate, ...

[Today's Paper](#) · [The Crossword](#) · [World News](#) · [Sports](#)

Google is your safe address bar

## **RULE#5: "Cookieless" default browser**

*Which browser will open  
the next random ingress link?*

16:10

94%



https://renfe.es@wpme.cc/J



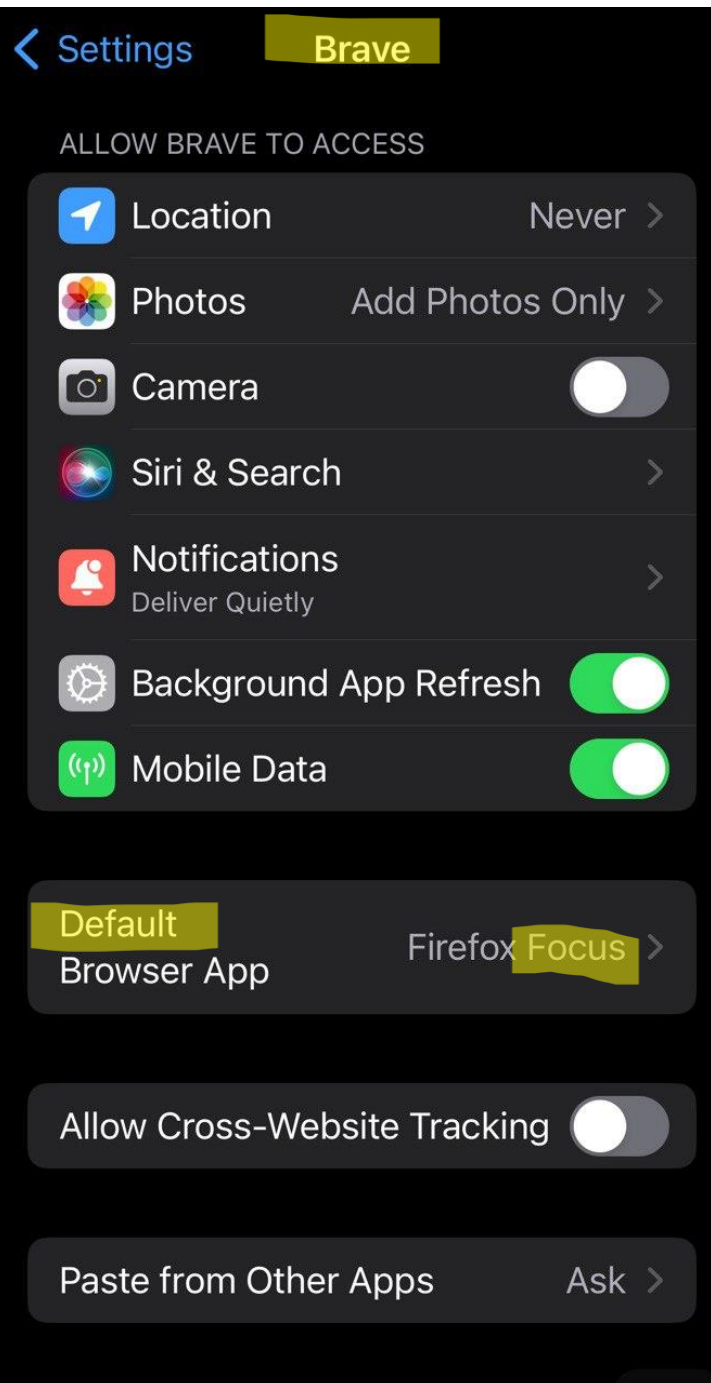
You are about to log in to the site "wpme.cc" with the username "renfe.es", but the website does not require authentication. This may be an attempt to trick you.

Is "wpme.cc" the site you want to visit?

CANCEL

OK

Not Chrome only is your friend



**Firefox Focus has no memory**

The End

