GrapheneOS
@GrapheneOS@grapheneos.social

We were contacted by a journalist at Le Parisien newspaper with this prompt:

> I am preparing an article on the use of your secure personal data phone solution by drug traffickers and other criminals. Have you ever been contacted by the police?

Nov 19, 2025, 11:56 AM · · Web

100 boosts · **2** quotes · **83** favorites

GrapheneOS
@GrapheneOS
10h

> Are you aware that some of your clients might be criminals? And how does the company manage this issue?

Absolutely no further details were provided about what was being claimed, who was making it or the basis for those being made about it. We could only provide a very generic response to this.

3

GrapheneOS
@GrapheneOS
10h

Our response was heavily cut down and the references to human rights organizations, large tech companies and others using GrapheneOS weren't included. Our response was in English was translated by them: "we have no clients or customers" was turned into "nous n'avons ni clients ni usagers", etc...

2

GrapheneOS
@GrapheneOS
10h

Search

Live feeds

About

Mastodon is the best way to keep up with what's happening.

Follow anyone across the fediverse and see it all in chronological order. No algorithms, ads, or clickbait in sight.

Create account

Login

GrapheneOS is a freely available open source privacy project. It's obtained from our website, not shady dealers in dark alleys and the "dark web". It doesn't have a marketing budget and we certainly aren't promoting it through unlisted YouTube channels and the other nonsense that's being claimed.

1

GrapheneOS 10h
@GrapheneOS

GrapheneOS has no such thing as the fake Snapchat feature that's described. What they're describing appears to be forks of GrapheneOS by shady companies infringing on our trademark. Those products may not even be truly based on GrapheneOS, similar to how ANOM used parts of it to pass it off as such.

1

GrapheneOS 10h
@GrapheneOS

France is an increasingly authoritarian country on the brink of it getting far worse. They're already very strong supporters of EU Chat Control. Their fascist law enforcement is clearly ahead of the game pushing outrageous false claims about open source privacy projects. None of it is substantiated.

2

GrapheneOS 10h
@GrapheneOS

iodéOS and /e/OS are based in France. iodéOS and /e/OS make devices dramatically more vulnerable while misleading users about privacy and security. These fake privacy products serve the interest of authoritarians rather than protecting people. /e/OS receives millions of euros in government funding.

3

GrapheneOS 10h
@GrapheneOS

Those lag many months to years behind on providing standard Android privacy and security patches. They heavily encourage users to use devices without working disk encryption and important security protections. Their users have their data up for grabs by apps, services and governments who want it.

1

GrapheneOS
@GrapheneOS
10h

There's a reason they're going after a legitimate privacy and security project developed outside of their jurisdiction rather than 2 companies based in France within their reach profiting from selling 'privacy' products.

discuss.grapheneos.org/d/24134...

Here's that article:

archive.is/AhMsj

GrapheneOS Discussion Forum
Devices lacking standard privacy...
GrapheneOS discussion forum

6

David Penfold
@davep@infosec.exchange
10h

@GrapheneOS They tried the same with some shoddy messenger service to replace Signal. It was truly woeful.

0

Niavy
@niavy@masto.bike
10h

@GrapheneOS
Okay, you're a stronger OS than the other Android-based ones, particularly regarding privacy and degoogling, but you often despise other projects despite their efforts and the alternative these offer.

I acknowledge your strong efforts but I don't like at all your "We are the one white angel, other projects don't reach our purity".

5

GrapheneOS 10h
@GrapheneOS

@niavy Both products are outright scams. They're extraordinarily insecure and non-private. They're putting users at risk and misleading them with repeated false claims about privacy and security. Each person misled into buying their products enriches them at the cost of those users being far less protected against apps, services and attackers than if they used an iPhone. They lack the most basic privacy and security. GrapheneOS is not remotely in the same space and is not a for-profit company.

3

GrapheneOS 10h
@GrapheneOS

@niavy You should read the detailed information in discuss.grapheneos.org/d/24134... and the linked third party articles. It's not an exaggeration to refer to both /e/ and iodéOS as scams. They're fooling people into believing they're getting privacy when they're throwing it away compared to if they used an iPhone. It's very much in the interested of authoritarian governments for people to opt-in to having highly insecure devices which can be easily broken into both remotely and with physical access.

GrapheneOS Discussion Forum
Devices lacking standard privacy...
GrapheneOS discussion forum

1

kit 4h
@hypostase@bsd.network

@GrapheneOS @niavy The single thing that keeps me away from Graphene (apart from refusing to use a Pixel) is the cognitive load generated by trying to determine whether the FUD, loud as it is, is or is not valid.
It's very clear that graphene are very committed to a particular security model. It's less clear whether that security model meets my particular use-case, nor how to determine whether it might become so in the future, without all the shouting.

2

Libre>Gratis 3h
@libreovergratis@mastodon.social

@hypostase @GrapheneOS @niavy If you can't determine whether or not it meets your use case, it doesn't. You'll just be a headache for forum moderation.

1

kit 2h
@hypostase@bsd.network

@libreovergratis @GrapheneOS @niavy I know it doesn't :) because they very loudly dump on everybody else.

1

Libre>Gratis 2h
@libreovergratis@mastodon.social

@hypostase @GrapheneOS @niavy
The Internet: 'We need vocal privacy advocates and commited devs. '

advocates for privacy

The internet: 'Okay okay shut up already, gosh.'

1

kit 1h
@hypostase@bsd.network

@libreovergratis @GrapheneOS @niavy And a critical part of that is to have multiple models. If each is just trying to be the next monoculture, then the problem will not be solved.

For me, the critical factor is not having to use a US based service or product. Under e/os that's painful, Calyx is currently out of play, Graphene is ruled out for hardware, and their rhetoric seems to reach somewhat beyond what it can support.

My claim is that when rhetoric is not clearly backed up, then only those who have the time and will to see past it, might be able to come to a place of trust.

So far I have not really seen a good and neutral analysis of the architectural choices of each of the projects. Just people shouting.

1

Libre>Gratis 1h
@libreovergratis@mastodon.social

@hypostase @GrapheneOS @niavy the neutral analysis you're looking for is easily accessible, but instead you simply choose to shout back.

And yes I agree that multiple models are important, and after much research I found the model I determined to be far superior, believe me I didn't want to give Google any more of my money for the required hardware, but it was well worth the compromise IMO.

1

kit 1h
@hypostase@bsd.network

@libreovergratis @GrapheneOS @niavy I have read several analyses. So far none have matched the rhetoric. Nevertheless I understand that their model works for many, just not for me.

1

Libre>Gratis 1h
@libreovergratis@mastodon.social

@hypostase @GrapheneOS @niavy I'm still not sure what rhetoric you're referring to, I've yet to find a single undelivered promise.

Regardless I wish you luck in finding an AOSP fork that works for you, unfortunately you might just have to roll your own to get everything you want.

0

GrapheneOS
@GrapheneOS
55m

@hypostase @niavy We're defending ourselves from major ongoing attacks on our project/team. We're not shouting.

GrapheneOS is a privacy project. It provides substantial privacy improvements including Contact Scopes, Storage Scopes, Sensors toggle, per-connection Wi-Fi anonymity including but not limited to MAC randomization, fixes for 5 different Android VPN leaks and far more. Privacy depends on security so we also heavily focus on that with exploit protections, which are proven to work well.

1

kit
@hypostase@bsd.network
37m

@GrapheneOS @niavy When you use words like ”scam” it starts to look less like defence. Defence would look like ”x said thing a and we disagree because … ”

For some of us our model may be different. Personally, for me, my model specifically excludes the use of google accounts, and it’s not clear to me that that would be possible with graphene, even leaving aside the hardware issue.

Because I have a particular set of priorities, I find it difficult to see a justification for the word ”scam” in some instances.

On the other hand, I have not seen any project that looks like it might meet my needs, and won’t until, and unless, there is strong support for non-US, preferably under multiple jurisdictions, third-party app suppliers for critical apps. That, of course, is beyond the scope of a single project, no matter how necessary it may be.

1

GrapheneOS
@GrapheneOS
3m

@hypostase @niavy Unlike both of those operating systems, GrapheneOS doesn't connect to any Google servers by default and does not contain privileged Google service integration into the OS. We don't market it by calling it "degoogled" since the point if strong privacy and security, not avoiding one particular set of services.

Read discuss.grapheneos.org/d/24134... and the information from the Divested Computing project we have linked there. Calling that a scam is completely and thoroughly justified.

GrapheneOS Discussion Forum

Devices lacking standard privacy...

GrapheneOS discussion forum

1

GrapheneOS
@GrapheneOS
2m

@hypostase @niavy GrapheneOS uses the only available secure hardware with support for installing another OS. We aren't going to massively lower those standards and start using devices without working disk encryption, important exploit protections needed to keep commercial exploit tools and other attackers out and basic privacy/security patches for the firmware/drivers. Not having proper privacy/security patches is near universal across Android devices and rules out most hardware by itself.

1

GrapheneOS
@GrapheneOS
56s

@hypostase @niavy Do you think that it's okay for /e/ to have what they advertise as a private speech-to-text which instead of doing processing locally sends the user's speech data to OpenAI without ever asking for consent? It's hidden away in the privacy policy. When confronted about it, they falsely claimed the data is anonymized which is not true. They just run it through their servers first. /e/ and Murena have MANY cases like this with the apps/services. It's the tip of the iceberg though.

1

GrapheneOS
@GrapheneOS
now

@hypostase @niavy They go many weeks and months without providing basic privacy/security patches on a regular basis. They lag substantially far behind on OS releases which means not ever having the full set of patches since they're always behind and relying on the partial backports Google does for only vulnerabilities they deem High and Critical severity. Google considers most privacy issues Moderate or Low severity so they're not backported and /e/ doesn't get the fixes until years later.

1

GrapheneOS
@GrapheneOS
now

@hypostase @niavy Android provides full privacy and security support for the latest release of the OS. Older releases of the OS get partial backports. Being on older releases also means missing current generation protections. Privacy and security are moving targets and Android is not staying ahead of what's needed for reasonable privacy and security, which means being far behind on the patches and protections makes things a lot worse. Privacy and security are bad enough on up-to-date software.

0

Zahox
@zahox@mastodon.social
8h

@GrapheneOS I was always wondering if Play Store is a more secure way on GrapheenOS to get apps, than Obtainium with Github/Codeberg.

1

jjlinux | X unverified 😅
@linuxjj@mastodon.social
8h

@zahox @GrapheneOS in all those cases, you need to trust someone. For example, I've chosen to trust the F-Droid team, so I download from F-Droid. I Obtainium, I only use it to install apps from developers I already trust from github, Gitlab or Codeberg. The Play store is no different, I don't trust Google, so I avoid it like the plague as much as I can.

0

Niavy 10h
@niavy@masto.bike

@GrapheneOS
You may be talking about GrapheneOS scams ? As for me I am talking about LineageOS-based ROMs.
These are not as bad alternatives as you present them. OK, these are "weaker" than your ROM, but these also are better choices than stock ROMs.

2

GrapheneOS 10h
@GrapheneOS

@niavy Those are highly insecure and non-private. They do not provide basic privacy and security patches/protections. They lag many months and even years behind on providing basic privacy and security patches. They're flat out unsafe to use and remain vulnerable to attacks through vulnerabilities known to be exploited in the wild. Google publicly documents some of the exploits they take many months or even years to patch as being exploited in the wild, and they only have a little bit of insight.

2

LΞX/NØVΛ 🇪🇺 6h
@lexinova@toot.community

@GrapheneOS @niavy don't answer to him, it's a troll, or one of those who talk big while not understanding how hardware security work and think software can do anything.

Surly one of those that think that a software update to AI can create skynet....

2

Niavy 5h
@niavy@masto.bike

@lexinova
No, not at all. I hate LLM AI.
@GrapheneOS

1

LΞX/NØVΛ 🇪🇺 4h
@lexinova@toot.community

@niavy @GrapheneOS of a first degree guy ... cool

1

Niavy 4h
@niavy@masto.bike

@lexinova
Huh?
@GrapheneOS

0

Breizh 4h
@breizh@pleroma.breizh.pm

@lexinova @GrapheneOS @niavy Well, it's not a troll, only someone that don't know what is this thread about, and try to understand. But only receive blunt response, and now even rude ones. That's not helping...

2

Niavy 4h
@niavy@masto.bike

@breizh
You know me. They don't 😕
@GrapheneOS @lexinova

0

LΞX/NØVΛ 🇪🇺 4h
@lexinova@toot.community

@breizh @GrapheneOS @niavy lol making false claim is "try to understand" LMAO

1

Breizh 4h
@breizh@pleroma.breizh.pm

@lexinova @GrapheneOS @niavy Like he said, I know him. I think he didn't realise it was a false claim… it was more probably a genuine mistake.

1

LΞX/NØVΛ 🇪🇺
@lexinova@toot.community

4h

@breizh @GrapheneOS @niavy don't realising it is not an excuse even more when said like he said it.

When you are not sure you add thing like "correct me if i'm wrong but".

here it was not a question but an affirmation

2

Niavy
@niavy@masto.bike

4h *

@lexinova
OK so pointing out a superior "we're better" assertion feeling is a false claim ?
Saying while other ROMs may be worse than Graphene, these can be better than stock is a false claim ?

Whoa.
@breizh @GrapheneOS

3

LΞX/NØVΛ 🇪🇺
@lexinova@toot.community

4h *

@niavy @breizh @GrapheneOS and you continue to invent false information.

What they claim is not "we are better" they claim "other lie on their security".

1

Breizh
@breizh@pleroma.breizh.pm

4h

@lexinova @niavy @GrapheneOS He's not inventing it, he believes it…

1

GrapheneOS
@GrapheneOS
57m

@niavy @lexinova @breizh They're extraordinarily insecure and non-private. They're definitely much worse than an iPhone for privacy and security. They're much worse than the stock Pixel OS for security and the privacy is quite mixed. Stock Pixel OS is far ahead on patching privacy vulnerabilities and providing modern privacy features due to being on current AOSP, but has more invasive services bundled. /e/ and iodéOS both always use Google services and bundle privileged access for them though.

0

Breizh
@breizh@pleroma.breizh.pm
4h

@niavy @lexinova @GrapheneOS Actually, it is, yeah. Well, in some case it could be true (like when they replace outdated stock ROMs), but's generally, other ROMs are worse than the stock one in terms of security (about privacy it's a harder to say, since they fix some stock problems, but the security breaches can create more privacy problems than it's solving).

2

Niavy
@niavy@masto.bike
4h

@breizh
Now I really got the point. Thanks.
@GrapheneOS @lexinova

0

Steph à vélo
@stephavelo@masto.bike
1h

@breizh
thank you for the explanation, i rent a fairphone with /e/os with @cooperative_commown because i don't want my data to go to google, but i expected the security to be the same

@GrapheneOS @niavy @lexinova

0

Breizh
@breizh@pleroma.breizh.pm
4h

@lexinova @GrapheneOS @niavy You're talking about the part he said "You may be talking about GrapheneOS scams ?" I guess?

The question was here. Okay, after it's an affirmation but it's more like a formulation error.

And the response is, no, Graphene didn't talk about the scams, but they were really talking about Lineage and their forks.

2

LΞX/NØVΛ 🇪🇺
@lexinova@toot.community
4h

@breizh @GrapheneOS @niavy no it's not, stop trying to defend false claim, and lie.

And if you continue all you will win is being blocked by them

2

Breizh
@breizh@pleroma.breizh.pm
4h

@lexinova @GrapheneOS @niavy I'm not saying he's right. Just that he really think what he's saying is. And you're not using the right method to convince him.

1

Niavy
@niavy@masto.bike
4h

@lexinova
Me? No I won't.
@breizh @GrapheneOS

0

GrapheneOS
@GrapheneOS
51m

@breizh @niavy @lexinova We were talking about forks of LineageOS. LineageOS itself is significantly less problematic, although still definitely lags far behind on privacy and security patches, has the issue of setting an inaccurate Android security patch level inherited and made worse by the forks and rolls back parts of the privacy/security model. The forks of it bundled a bunch of invasive services and rolling back privacy and security further are a different level of problematic than it.

0

C.Suthorn :prn:
@Life_is@no-pony.farm
6h

@GrapheneOS@grapheneos.social @niavy@masto.bike Graphene and iOS are the most secure mobile OSs. But they can only be used on Pixel and Apple. Both are expensive even when refubished.. Not everyone can afford that. If someone can spend 50 to 100 euro (and already has power adapter, usb cable etc) on a new or refurbished mobile smart device, what should them do? Buy the newest device within the price frame and keep the stock OS? Or what else? Iode, calix, linux, e, lineage, harmony, fire, ...? What is the least worse choice?

0

2babcc
@2babcc@mastodon.social
6h

@niavy @GrapheneOS LineageOS has lower security than all stock systems because it does not recommend users relock the bootloader, leaving it unlocked by default, and contains numerous other security vulnerabilities. Regarding privacy protection, if you are completely ungoogled, its a little bit better than stock systems. But in my opinion, privacy doesn't exist if security doesn't exist.

1

GrapheneOS
@GrapheneOS
6h

@2babcc @niavy Locking the bootloader only accomplishes something if the OS has verified boot support intact which it doesn't.

It's far more important that it regularly lags significantly behind on standard privacy and security patches. For example, not having the Pixel kernel, firmware and driver patches for June 2025 and later until they ported to Android 16 in October 2025 as one way it ends up lagging behind. LineageOS is much less bad than the forks of it.

0

Xtreix
@Xtreix@infosec.exchange
7h

@niavy @GrapheneOS

"' you often despise other projects despite their efforts and the alternative these offer.

I acknowledge your strong efforts but I don't like at all your "We are the one white angel, other projects don't reach our purity"."

No, this is not the case, It's about defending against hostile for-profit projects that have been scammed users for years. GrapheneOS wouldn't even mention them if they weren't constantly spreading attacks and misinformation against GrapheneOS. /e/ and iodéOS allow easy access to user data by companies and governments, they have an agenda and they receive millions in funding from the EU, then they talk to you about so-called digital sovereignty when the goal is actually easier access to user data.

1

LΞX/NØVΛ 🇪🇺
@lexinova@toot.community
6h

@Xtreix @niavy @GrapheneOS no not from EU from France.

Right now majority of EU country are against those move, it's why Chat Control failed 2 time to enforce mandatory client side scanning.

1

jjlinux | X unverified 😅
@linuxjj@mastodon.social
8h

@niavy @GrapheneOS too bad you don't like it. That's a proven fact. Iodè and e/os are nothing but bloated forks of LineageOS, entirely profit-based, and lying about their capabilities while

phoning Google from the first boot. Just look it up. Ask any serious security expert, GOS is the one mobile OS that can keep you secure, and the most private (unless you decide to make it less private on your own).

1

LΞX/NØVΛ 🇪🇺 6h
@lexinova@toot.community

@linuxjj @niavy @GrapheneOS As CISO i would use nothing else than Graphene os, they still can increase their security in some aspect, but realistically until they are free from their reverse engineering they must do on each new device, they lack time to add them.

0

Okay...okay 9h
@OK_OK@social.tchncs.de

@niavy @GrapheneOS Sorry, but this is simply not true. The GOS team have always been very open when it has come to security merits of other manufacturers (e.g. Apple's iPhones) on the one hand and on the technical limitations of their own OS on the other hand (e.g. IMEI revelation to mobile networks or cellular location triangulation by the carrier).

0

Live feeds

About

Mastodon is the best way to keep up with what's happening.

Follow anyone across the fediverse and see it all in chronological order. No algorithms, ads, or clickbait in sight.

Login