

Forum:[Hack Forums](#)

Thread: [Using Telegram anonymously](#)

Penguin20245 - February 18, 2025, 9:25 am

Hello.

My main goal is to be able to use 4 telegram accounts, as anonymous as it gets. The primary idea is to control a number of groups and channels, with backups (that's why one account is going to be the main and the others secondary). My way of approaching it is:

I get 5 prepaid sim cards (bought by somebody else, different locations). I get two mobile phones. First is going to be the Hotspot mobile phone (HMP), the second will be the main mobile phone (MMP).

The HMP will be always connected to a VPN and the MMP will be connected to the HMP (the MMP traffic will be routed through first the HMP, then VPN, then Telegram). Then, on the MMP, we register the 4 SIM cards with accounts, which then are discarded and put away safely, in need of future activation.

Now, what my goal with anonymity is being safe from law enforcement, as my country is repressive when it comes to journalism about opposition. Therefore, we are going to follow the law enforcement (LE) perspective. On stumbling upon a channel or a group of mine, the cycle goes as follows:

1. Issuing a subpoena for Telegram to disclose the data about the owning accounts of the channel. There, Telegram gives out the initial registration number and the IP addresses, that were used to login. Now, LE has 2 hints to follow:

1.1 Initial registration number

1.1.1. „The SIM card is on the name of ..., it was last activated there, no call has been made, no nothing“ which could lead to

1.1.1.1 Physical interrogation with the guy, responsible for buying them

1.1.1.2. Physical overlook of the place that they were registered

1.2. VPN IP addresses (they were used with no-logs)

1.2.1. Dead end. There is no linkage between IP addresses and accounts.

I believe the one-time use of the cards and the following use of just a HMP, makes a good division.

So, if I could get any more information whether that is a good strategy and I think it's a good discussion to be made overall. What are the weak links? What mistakes during operation could be made which would lead to ruining everything? How could it be made better? Additional security measures? Feel free to comment on everything here.

[*] A few notes:

1. Device footprint, I get it, but even if they find that all the Telegram accounts are linked, I guess it isn't much helpful information

2. If you could suggest a secure method to ALWAYS have the HMP connected to the VPN, for me the weakest link seems the possibility of accidentally disconnecting and linking real IP address.

3. Woud like to know whether we are certain that Telegram is being real when it comes to sharing only IP address and phone number, as they say.

Epic - February 18, 2025, 9:39 am

In my opinion, the weakest link is probably telegram itself. Are you locked into using telegram? Or would something like xmpp, simplex, or signal get the job done?

As far as IP leaks, making sure your tunnels are set up correctly and are set to not allow connection without vpn, that should be reasonably secure.

Ensure your hotspot device does not have any vulnerabilities or security issues. I have heard of some hotspot devices that were less than "reasonably" secure.

Penguin20245 - February 18, 2025, 9:41 am

(Feb 18, 2025 10:39 AM)Epic Wrote: [\[CITE\]](#) In my opinion, the weakest link is probably telegram itself. Are you locked into using telegram? Or would something like xmpp, simplex, or signal get the job done?Yes, locked into using it. It really isn't because of the messaging, but mostly about the channels.

(Feb 18, 2025 10:39 AM)Epic Wrote: [\[CITE\]](#) As far as IP leaks, making sure your tunnels are set up correctly and are set to not allow connection without vpn, that should be reasonably secure. Can you suggest a VPN? From my research, I see Mullvad as N1.

(Feb 18, 2025 10:39 AM)Epic Wrote: [\[CITE\]](#) Ensure your hotspot device does not have any vulnerabilities or security issues. I have heard of some hotspot devices that were less than "reasonably" secure.This is on point. I was thinking about the hotspot device. Any ideas? It could be a "cookie" router, a normal mobile phone, a mobile phone running Graphene, all kind of things. Also, keep in mind, we have a budget.

Epic - February 18, 2025, 9:51 am

(Feb 18, 2025 10:41 AM)Penguin20245 Wrote: [\[CITE\]](#) Yes, locked into using it. It really isn't because of the messaging, but mostly about the channels.

Can you suggest a VPN? From my research, I see Mullvad as N1.

This is on point. I was thinking about the hotspot device. Any ideas? It could be a "cookie" router, a normal mobile phone, a mobile phone running Graphene, all kind of things. Also, keep in mind, we have a budget.

VPN: from my experience and research, Mullvad, Proton, and IPVN are the most reputable. Mullvad offers anonymous payment methods, I am not sure if Proton and IVPN do though.

I can't offer much specific advice regarding telegram, as I don't use the platform.

I have heard good things about GL.iNet products, but have not used them myself, so I can't fully vouch. They have quite the selection of mobile routers and hotspots.

I will also give a massive +1 to GraheneOS. It is my daily driver (personal device). Posting from it right now. In my opinion, it doesn't make sense to anything that is sensitive on anything other than Graphene. The tech is top tier in my opinion.