

Forum: [Hack Forums](#)

Thread: [Because Jail Is NO Fun In Any Country | OPSEC GUIDE](#)

Chorozone - February 26, 2025, 1:17 am

Because Jail Is NO Fun In Any Country | OPSEC GUIDE

This comprehensive guide covers every aspect of operational security, from securing your internet connection and communications to protecting your financial transactions and staying safe offline. It's designed to help you stay invisible while making a difference. Obviously you have to become acquainted with the tools and practices i mention to avoid threats but this is a good start and relevant to anyone that has OPSEC questions or is at risk of surveillance

Quote: "The best way to stay invisible is to never be seen in the first place."
— Attributed to Edward Snowden

1. [b]Internet Connectivity: Staying Off the Radar

Your internet connection is one of the most vulnerable points in your digital footprint. Here's how to minimize risks:

Avoid Using Your Own Internet

Using your home or work internet can easily link activities back to you. Instead, consider these alternatives:

Mobile Hotspots

Purchase Prepaid SIM Cards : Buy prepaid SIM cards in cash at stores that don't require identification (e.g., gas stations, convenience stores).

Set Up Mobile Hotspots : Use these SIMs in a burner phone or dedicated hotspot device. Avoid linking them to your real identity.

Rotate Regularly : Change SIM cards periodically to avoid creating patterns.

Public Wi-Fi

Use Cafes, Libraries, or Parks : Connect to public Wi-Fi networks where possible. Avoid logging into accounts tied to your real identity.

Encrypt Traffic : Always use encryption tools like Tor or a trusted, open-source VPN (e.g., ProtonVPN, Mullvad) when on public Wi-Fi.

Physical Distance : Perform sensitive operations far away from your home or workplace to reduce geolocation risks.

Additional Tips

Disable GPS : Turn off location services on all devices to prevent tracking.

Use Signal App : For encrypted messaging, use Signal and disable location sharing.

2. Tails OS: A Portable Fortress

Tails (The Amnesic Incognito Live System) is a privacy-focused operating system that leaves no trace on the host computer. It routes all internet traffic through Tor by default.

Why Use Tails?

- Encrypts all internet traffic through Tor.
- Prevents data storage on the host computer.
- Can be run entirely from a USB drive without leaving traces.

Setup Instructions

Download Tails : Visit the official website (tails.boum.org) over a secure connection.

Verify Download : Check the download signature using GPG to ensure authenticity.

Install on USB : Use the official installer to create a bootable USB stick.

Boot Securely : Restart your computer and boot from the USB stick. Disable network connections until Tails loads.

Best Practices

Persistent Storage : Use persistent storage only if necessary, and encrypt it with a strong password.

Regular Updates : Keep Tails updated to patch vulnerabilities.

Separate Tasks : Never mix sensitive and non-sensitive tasks within the same Tails session.

3. Online OPSEC: Protecting Your Digital Footprint

Online operational security involves protecting your identity, behavior, and metadata. Even small details can reveal who you are.

Key Principles

Don't Reveal Personal Details

Avoid sharing names, addresses, phone numbers, email addresses, or anything else that could identify you.

Be cautious about indirect details such as hobbies, favorite books, or places you frequent.

Humanize Your Writing

People may analyze your writing style, vocabulary, grammar, and punctuation to figure out who you are.

Use tools like Dandelion Sprout's Anonymizer to randomize your text.

Vary sentence structure and word choice to avoid consistent patterns.

Strip Metadata

Files often carry metadata (hidden information) that can reveal their origin.

Use tools like Metadata Cleaner (built into Tails) to strip metadata before sharing files.

Be Consistent

Maintain consistent behavior across platforms so you don't draw attention.

Avoid posting during times that might reveal your location or routine (e.g., late-night posts if you normally sleep early).

Password Management

Never Reuse Passwords : One of the biggest mistakes people make is reusing passwords across accounts. This was the downfall of Cracked.io, where the admin used the same credentials for personal and professional life. When those passwords appeared in a breach, it led to the site being compromised.

Use Strong, Unique Passwords : Aim for at least 16 characters combining letters, numbers, and symbols.

Password Managers : Use a reputable password manager like Bitwarden, KeePassXC, or 1Password to generate and store complex passwords securely.

Enable Two-Factor Authentication (2FA) : Prefer authenticator apps (e.g., Google Authenticator, Authy) over SMS-based 2FA.

Social Engineering Defense

Be wary of phishing attempts and social engineering tactics aimed at tricking you into revealing information.

Assume everyone you interact with online could potentially be an adversary.

4. Tor & Whonix: Navigating the Web Anonymously

Tor and Whonix are essential tools for maintaining anonymity online.

Tor: The Onion Router

Tor routes your internet traffic through multiple layers of encryption, making it nearly impossible to trace.

How to Use Tor

Download Tor Browser : Get it from the official site (www.torproject.org).

Verify Download : Verify the signature to ensure authenticity.

Configure Settings : Disable JavaScript if needed, and always access websites over HTTPS.

Important Notes

Avoid Torrenting : Torrenting uses too much bandwidth and increases the risk of deanonymization.

Use Bridges : If your ISP blocks Tor traffic, use bridges provided by the Tor Project.

Combining Tor with a VPN

If you're concerned about your ISP seeing that you're connecting to Tor, consider using a VPN-TOR setup . This way, your ISP sees only the encrypted connection to the VPN server, which then routes your traffic into Tor.

? Warning : Do NOT use a VPN inside Tor. This creates unnecessary complexity and can actually weaken your anonymity. Stick to either Tor alone or a clean VPN-TOR setup.

Whonix: The Ultimate Privacy Tool

Whonix takes Tor to the next level by running everything inside two virtual machines: one for networking (Whonix-Gateway) and one for applications (Whonix-Workstation). All traffic is automatically routed through Tor.

Benefits of Whonix

- Isolates your workstation from direct internet exposure.

- Protects against IP leaks and DNS leaks.

- Provides a sandboxed environment where even malware would struggle to compromise your real identity.

Setup Instructions

- Download Whonix from whonix.org .

- Install it in VirtualBox or Qubes OS.

- Boot both the Gateway and Workstation VMs and configure as needed.

Tips for Using Tor and Whonix

- Avoid torrenting over Tor due to bandwidth issues and potential deanonymization risks.

- Combine Whonix with Tails for maximum protection.

5. Monero: Securing Your Financial Transactions

Monero is a privacy-focused cryptocurrency that provides strong transactional anonymity compared to Bitcoin.

Why Use Monero?

- Transactions are untraceable thanks to ring signatures and stealth addresses.

- No public ledger showing sender/receiver relationships.

- Minimizes metadata leakage.

Running Your Own Monero Node

Having your own Monero node gives you more control and privacy. Instead of relying on third-party services that might track your activity, you become part of the decentralized network.

Steps to Set Up a Monero Node

- Download Monero Core software from getmonero.org .

- Install it on a secure machine or server.

Sync the blockchain, which may take some time depending on hardware and internet speed.
Use the node locally for wallet synchronization and transactions.

Additional Tips

Store Monero in cold storage wallets for long-term holding.

Avoid reusing addresses; always generate new ones for each transaction.

Consider using Kovri (a project aiming to integrate I2P routing with Monero) if available, for extra privacy.

6. Secure Communication Methods: Staying in Touch Safely

Communication is critical but also risky. Choose tools that prioritize end-to-end encryption and minimal metadata collection.

Recommended Tools

Signal

Overview : Signal is widely regarded as the gold standard for secure messaging. It offers strong end-to-end encryption, voice/video calls, and disappearing messages.

Key Features :

- Open-source and audited for security.

- Minimal metadata collection.

- Available on desktop and mobile devices.

Best Practices :

- Use a burner phone number if possible.

- Disable screenshots in the app settings.

- Enable disappearing messages for sensitive conversations.

Threema

Overview : Threema allows users to remain completely anonymous by creating an account without a phone number.

Key Features :

- End-to-end encryption.

- Anonymous registration (no phone number required).

- Supports file sharing and group chats.

Best Practices :

- Use a pseudonymous identity when registering.

- Avoid linking Threema to your real email address or phone number.

Jitsi Meet / Jabber (XMPP)

Overview : Jitsi Meet and Jabber provide secure video conferencing and instant messaging with end-to-end encryption.

Key Features :

- Fully open-source and decentralized.
- No account creation required for Jitsi Meet.
- Compatible with various clients like Conversations and Gajim.

Best Practices :

- Host your own Jitsi server for maximum control.
- Use OMEMO for end-to-end encryption in Jabber clients.

Tox

Overview : Tox is a peer-to-peer encrypted communication platform that doesn't rely on centralized servers.

Key Features :

- End-to-end encryption for text, voice, and video calls.
- Decentralized architecture.
- No need for accounts or phone numbers.

Best Practices :

- Share your Tox ID securely (e.g., via Tails or Tor).
- Regularly update the client to patch vulnerabilities.

Avoid These Tools

Telegram

Why It's Bad OPSEC :

- Only secret chats are end-to-end encrypted; regular chats lack proper encryption.
- Collects significant amounts of metadata, including IP addresses and device information.
- Centralized architecture makes it vulnerable to government requests or hacking attempts.

Alternative Recommendation : Use Signal or Threema instead.

Other Insecure Platforms

WhatsApp : While WhatsApp does offer end-to-end encryption, its ties to Facebook raise privacy concerns. Metadata is still collected, and backups may not be encrypted.

Facebook Messenger/SMS : These platforms lack end-to-end encryption entirely and should never be used for sensitive communications.

7. Physical Security: Protecting Yourself Offline

Digital security is only half the battle. You must also safeguard yourself physically.

Key Steps

Avoid Surveillance

Don't discuss sensitive topics in public. Use a burner phone for coordination.

Cover cameras/mics with tape when not in use.

Emergency Plans

Have a “burner” identity ready with fake documents .

Destroy Evidence

Use tools like DBAN (Darik's Boot and Nuke) to wipe hard drives before disposal.

8. Final Checks: Audit Your OPSEC

Regularly review your operational security practices to ensure they're effective.

Test for Leaks

Use tools like Am I Unique? (in Tails) to check for browser fingerprinting risks.

Or Move to France Apparently they don't care and let you have women in jail [Bastille](#)
(Sarcasm is implied)

Discussions Below Is Encouraged

Chorozon - February 26, 2025, 1:22 am

(Feb 26, 2025 02:17 AM)Virulent Wrote: [\[CITE\]](#) This is an incredibly high quality guide [Chorozon](#).

All members of our Cyber community are now safer from the Federalis having read it.

Thanks man ! i have noticed a massive hole in just practical OPSEC guides and practices on this forum

I hope everyone takes a read and stays safe and anonymous and away from the Glowboys

Bastille - February 26, 2025, 3:27 am

Thanks for this guide, but jail is actually fun in France, you can have a playstation and a TV, you can cook, you even go to museums etc. This country is a fucking joke ?

Chorozon - February 26, 2025, 3:59 am

(Feb 26, 2025 04:27 AM)Bastille Wrote: [\[CITE\]](#) Thanks for this guide, but jail is actually fun in France, you can have a playstation and a TV, you can cook, you even go to museums etc. This country is a fucking joke ?

But can you have women ?

(Feb 26, 2025 04:27 AM)Bastille Wrote: [\[CITE\]](#) Thanks for this guide, but jail is actually fun in France, you can have a playstation and a TV, you can cook, you even go to museums etc. This country is a fucking joke ?

I seen what france did to Pavel Durov , France is not chill.??

Bastille - February 26, 2025, 4:09 am

(Feb 26, 2025 04:59 AM)Chorozon Wrote: [\[CITE\]](#) But can you have women ?

I seen what france did to Pavel Durov , France is not chill.??

Yes you can have women, France is chill regarding prisoners / jail

This comprehensive guide covers every aspect of operational security, from securing your internet connection and communications to protecting your financial transactions and staying safe offline. It's designed to help you stay invisible while making a difference. Obviously you have to become acquainted with the tools and practices i mention to avoid threats but this is a good start and relevant to anyone that has OPSEC questions or is at risk of surveillance

1. [b]Internet Connectivity: Staying Off the Radar

Your internet connection is one of the most vulnerable points in your digital footprint. Here's how to minimize risks:

Avoid Using Your Own Internet

Using your home or work internet can easily link activities back to you. Instead, consider these alternatives:

Mobile Hotspots

Purchase Prepaid SIM Cards : Buy prepaid SIM cards in cash at stores that don't require identification (e.g., gas stations, convenience stores).

Set Up Mobile Hotspots : Use these SIMs in a burner phone or dedicated hotspot device. Avoid linking them to your real identity.

Rotate Regularly : Change SIM cards periodically to avoid creating patterns.

Public Wi-Fi

Use Cafes, Libraries, or Parks : Connect to public Wi-Fi networks where possible. Avoid logging into accounts tied to your real identity.

Encrypt Traffic : Always use encryption tools like Tor or a trusted, open-source VPN (e.g., ProtonVPN, Mullvad) when on public Wi-Fi.

Physical Distance : Perform sensitive operations far away from your home or workplace to reduce geolocation risks.

Additional Tips

Disable GPS : Turn off location services on all devices to prevent tracking.

Use Signal App : For encrypted messaging, use Signal and disable location sharing.

2. Tails OS: A Portable Fortress

Tails (The Amnesic Incognito Live System) is a privacy-focused operating system that leaves no trace on the host computer. It routes all internet traffic through Tor by default.

Why Use Tails?

- Encrypts all internet traffic through Tor.
- Prevents data storage on the host computer.
- Can be run entirely from a USB drive without leaving traces.

Setup Instructions

- Download Tails : Visit the official website (tails.boum.org) over a secure connection.
- Verify Download : Check the download signature using GPG to ensure authenticity.
- Install on USB : Use the official installer to create a bootable USB stick.
- Boot Securely : Restart your computer and boot from the USB stick. Disable network connections until Tails loads.

Best Practices

- Persistent Storage : Use persistent storage only if necessary, and encrypt it with a strong password.
- Regular Updates : Keep Tails updated to patch vulnerabilities.
- Separate Tasks : Never mix sensitive and non-sensitive tasks within the same Tails session.

3. Online OPSEC: Protecting Your Digital Footprint

Online operational security involves protecting your identity, behavior, and metadata. Even small details can reveal who you are.

Key Principles

Don't Reveal Personal Details

Avoid sharing names, addresses, phone numbers, email addresses, or anything else that could identify you.

- Be cautious about indirect details such as hobbies, favorite books, or places you frequent.

Humanize Your Writing

People may analyze your writing style, vocabulary, grammar, and punctuation to figure out who you are.

- Use tools like Dandelion Sprout's Anonymizer to randomize your text.

- Vary sentence structure and word choice to avoid consistent patterns.

Strip Metadata

Files often carry metadata (hidden information) that can reveal their origin.

- Use tools like Metadata Cleaner (built into Tails) to strip metadata before sharing files.

Be Consistent

Maintain consistent behavior across platforms so you don't draw attention.

- Avoid posting during times that might reveal your location or routine (e.g., late-night posts if you

normally sleep early).

Password Management

Never Reuse Passwords : One of the biggest mistakes people make is reusing passwords across accounts. This was the downfall of Cracked.io, where the admin used the same credentials for personal and professional life. When those passwords appeared in a breach, it led to the site being compromised.

Use Strong, Unique Passwords : Aim for at least 16 characters combining letters, numbers, and symbols.

Password Managers : Use a reputable password manager like Bitwarden, KeePassXC, or 1Password to generate and store complex passwords securely.

Enable Two-Factor Authentication (2FA) : Prefer authenticator apps (e.g., Google Authenticator, Authy) over SMS-based 2FA.

Social Engineering Defense

Be wary of phishing attempts and social engineering tactics aimed at tricking you into revealing information.

Assume everyone you interact with online could potentially be an adversary.

4. Tor & Whonix: Navigating the Web Anonymously

Tor and Whonix are essential tools for maintaining anonymity online.

Tor: The Onion Router

Tor routes your internet traffic through multiple layers of encryption, making it nearly impossible to trace.

How to Use Tor

Download Tor Browser : Get it from the official site (www.torproject.org).

Verify Download : Verify the signature to ensure authenticity.

Configure Settings : Disable JavaScript if needed, and always access websites over HTTPS.

Important Notes

Avoid Torrenting : Torrenting uses too much bandwidth and increases the risk of deanonymization.

Use Bridges : If your ISP blocks Tor traffic, use bridges provided by the Tor Project.

Combining Tor with a VPN

If you're concerned about your ISP seeing that you're connecting to Tor, consider using a VPN-TOR setup . This way, your ISP sees only the encrypted connection to the VPN server, which then routes your traffic into Tor.

? **Warning :** Do NOT use a VPN inside Tor. This creates unnecessary complexity and can actually

weaken your anonymity. Stick to either Tor alone or a clean VPN-TOR setup.

Whonix: The Ultimate Privacy Tool

Whonix takes Tor to the next level by running everything inside two virtual machines: one for networking (Whonix-Gateway) and one for applications (Whonix-Workstation). All traffic is automatically routed through Tor.

Benefits of Whonix

- Isolates your workstation from direct internet exposure.

- Protects against IP leaks and DNS leaks.

- Provides a sandboxed environment where even malware would struggle to compromise your real identity.

Setup Instructions

- Download Whonix from whonix.org.

- Install it in VirtualBox or Qubes OS.

- Boot both the Gateway and Workstation VMs and configure as needed.

Tips for Using Tor and Whonix

- Avoid torrenting over Tor due to bandwidth issues and potential deanonymization risks.

- Combine Whonix with Tails for maximum protection.

5. Monero: Securing Your Financial Transactions

Monero is a privacy-focused cryptocurrency that provides strong transactional anonymity compared to Bitcoin.

Why Use Monero?

- Transactions are untraceable thanks to ring signatures and stealth addresses.

- No public ledger showing sender/receiver relationships.

- Minimizes metadata leakage.

Running Your Own Monero Node

Having your own Monero node gives you more control and privacy. Instead of relying on third-party services that might track your activity, you become part of the decentralized network.

Steps to Set Up a Monero Node

- Download Monero Core software from getmonero.org.

- Install it on a secure machine or server.

- Sync the blockchain, which may take some time depending on hardware and internet speed.

- Use the node locally for wallet synchronization and transactions.

Additional Tips

- Store Monero in cold storage wallets for long-term holding.

Avoid reusing addresses; always generate new ones for each transaction.

Consider using Kovri (a project aiming to integrate I2P routing with Monero) if available, for extra privacy.

6. Secure Communication Methods: Staying in Touch Safely

Communication is critical but also risky. Choose tools that prioritize end-to-end encryption and minimal metadata collection.

Recommended Tools

Signal

Overview : Signal is widely regarded as the gold standard for secure messaging. It offers strong end-to-end encryption, voice/video calls, and disappearing messages.

Key Features :

- Open-source and audited for security.
- Minimal metadata collection.
- Available on desktop and mobile devices.

Best Practices :

- Use a burner phone number if possible.
- Disable screenshots in the app settings.
- Enable disappearing messages for sensitive conversations.

Threema

Overview : Threema allows users to remain completely anonymous by creating an account without a phone number.

Key Features :

- End-to-end encryption.
- Anonymous registration (no phone number required).
- Supports file sharing and group chats.

Best Practices :

- Use a pseudonymous identity when registering.
- Avoid linking Threema to your real email address or phone number.

Jitsi Meet / Jabber (XMPP)

Overview : Jitsi Meet and Jabber provide secure video conferencing and instant messaging with end-to-end encryption.

Key Features :

- Fully open-source and decentralized.
- No account creation required for Jitsi Meet.
- Compatible with various clients like Conversations and Gajim.

Best Practices :

- Host your own Jitsi server for maximum control.

Use OMEMO for end-to-end encryption in Jabber clients.

Tox

Overview : Tox is a peer-to-peer encrypted communication platform that doesn't rely on centralized servers.

Key Features :

- End-to-end encryption for text, voice, and video calls.
- Decentralized architecture.
- No need for accounts or phone numbers.

Best Practices :

- Share your Tox ID securely (e.g., via Tails or Tor).
- Regularly update the client to patch vulnerabilities.

Avoid These Tools

Telegram

Why It's Bad OPSEC :

- Only secret chats are end-to-end encrypted; regular chats lack proper encryption.
- Collects significant amounts of metadata, including IP addresses and device information.
- Centralized architecture makes it vulnerable to government requests or hacking attempts.

Alternative Recommendation : Use Signal or Threema instead.

Other Insecure Platforms

WhatsApp : While WhatsApp does offer end-to-end encryption, its ties to Facebook raise privacy concerns. Metadata is still collected, and backups may not be encrypted.

Facebook Messenger/SMS : These platforms lack end-to-end encryption entirely and should never be used for sensitive communications.

7. Physical Security: Protecting Yourself Offline

Digital security is only half the battle. You must also safeguard yourself physically.

Key Steps

Avoid Surveillance

- Don't discuss sensitive topics in public. Use a burner phone for coordination.
- Cover cameras/mics with tape when not in use.

Emergency Plans

Have a "burner" identity ready with fake documents .

Destroy Evidence

Use tools like DBAN (Darik's Boot and Nuke) to wipe hard drives before disposal.

8. Final Checks: Audit Your OPSEC

Regularly review your operational security practices to ensure they're effective.

Test for Leaks

Use tools like Am I Unique? (in Tails) to check for browser fingerprinting risks.

Or Move to France Apparently they don't care and let you have women in jail [Bastille](#)
(Sarcasm is implied)

Discussions Below Is Encouraged

(Feb 26, 2025 05:09 AM)Bastille Wrote: [\[CITE\]](#) Yes you can have women, France is chill regarding prisoners / jail

The guide has been updated to accommodate your out of the box suggestion for OPSEC ?????

tkboom - February 26, 2025, 6:32 am

Chorozon you are a fickle person. I don't know why you gave me a bad review. Did I offend you?

Chorozon - February 26, 2025, 6:41 am

(Feb 26, 2025 07:32 AM)tkboom Wrote: [\[CITE\]](#) Chorozon you are a fickle person. I don't know why you gave me a bad review. Did I offend you?

Hack Forums has a feature where i can award people negative reputation if i think they are LQ members and because i am pretty sure your a researcher trying to SE people into a honey trap or your just a bizarre person who actually spams random LQ stuff around the forum

So i awarded you the No rats, no snitches, no bitches. with a negative -3 because thats what i think you are

You have outlined my point by bringing this up in a unrelated thread and also dming me

tkboom - February 26, 2025, 7:26 am

(Feb 26, 2025 07:41 AM)Chorozon Wrote: [\[CITE\]](#) Hack Forums has a feature where i can award people negative reputation if i think they are LQ members and because i am pretty sure your a researcher trying to SE people into a honey trap or your just a bizarre person who actually spams random LQ stuff around the forum

So i awarded you the No rats, no snitches, no bitches. with a negative -3 because thats what i think you are

You have outlined my point by bringing this up in a unrelated thread and also dming me

What evidence do you have? Are you just labeling others based on your own assumptions?

I am not, and I don't accept your way either! I am very angry!

If you don't have the ability, you don't have to do .

And we're just communicating, you haven't done anything yet.

You are the one who deleted the chat history. You are also the one who made negative comments!

Do you think this is good?

Spikkeljuan - February 26, 2025, 9:11 am

(Feb 26, 2025 08:26 AM)tkboom Wrote: [\[CITE\]](#) What evidence do you have? Are you just labeling others based on your own assumptions?

I am not, and I don't accept your way either! I am very angry!

If you don't have the ability, you don't have to do .
And we're just communicating, you haven't done anything yet.
You are the one who deleted the chat history. You are also the one who made negative comments!
Do you think this is good?
Bruh do this shit in DM's or sum
Love the guide!
Is there anyway i can get an PDF of this?
Also would a proxy chains be over the top when using Tor just like you'd described?

Chorozon - February 26, 2025, 11:26 pm

(Feb 26, 2025 10:11 AM)Spikkeljuan Wrote: [\[CITE\]](#) Bruh do this shit in DM's or sum
Love the guide!
Is there anyway i can get an PDF of this?
Also would a proxy chains be over the top when using Tor just like you'd described?
Thanks bro <3
I might do a more involved version as a PDF i didn't want to go to deep and actually mess up some peoples opsec practices
I usually reserve proxychains for CLI tasks for specific actions like scanning so i would use residential proxys on a vm or VPS

stillworking247 - February 28, 2025, 7:56 pm

Thanx for all the free info <3

some new tips i didn't know!

Just4kickz - March 14, 2025, 8:21 pm

Still currently reading but get into this before before downloading or doing anything illegal. Big Bump

Chorozon - March 15, 2025, 3:34 am

(Mar 14, 2025 08:21 PM)Just4kickz Wrote: [\[CITE\]](#) Still currently reading but get into this before before downloading or doing anything illegal. Big Bump
Thanks man glad your getting the knowledge
I would recommend reading all my threads before anyone does anything naughty on the web

Just4kickz - March 15, 2025, 3:37 am

(Mar 14, 2025 08:21 PM)Just4kickz Wrote: [\[CITE\]](#) Still currently reading but get into this before before downloading or doing anything illegal. Big Bump
No worries, I'll be sure to have a read. Thanks again!

HerrWinston - May 9, 2025, 1:26 am

Loved it, awesome thread

gnojedkire - May 9, 2025, 2:29 pm

Wooo , Thanks for this über handbook!

s1m0nc - June 21, 2025, 8:45 am

Thank you for sharing. I learned a lot.

nakedshaman - June 22, 2025, 9:22 am

This is amazing. Thank you immensely for this guide. Kudos

Gawin - June 29, 2025, 10:47 am

Incredible guide, the most comprehensive I've ever seen, thank you.

Chorozon - July 14, 2025, 8:40 pm

Part 2 is coming soon guys

immeiron - July 15, 2025, 12:04 am

What about webrtc and dns leaks? They can unmask you real ip identity

Chorozon - July 15, 2025, 12:15 am

(Jul 15, 2025 12:04 AM)immeiron Wrote: [\[CITE\]](#) What about webrtc and dns leaks? They can unmask you real ip identity

If you check chapter 1 line 1 i talk about how using your own network is a security risk and your "freedom fighting" should never be done on a network connected to your true identity

Tyr - July 15, 2025, 12:24 am

Or just stay away from posting proper OPSEC guides on a website such as this which everybody knows logs your IP into a centralized database to then migrate to the cloud/data-brokers for further enhancement and refinement of your digitally unique identifier and unique digital thumbprint to better understand who you are to provide you with targeted ads based on your geodata

haha. i only joke. Thanks for your contribution here.

Chorozon - July 15, 2025, 12:27 am

(Jul 15, 2025 12:24 AM)Tyr Wrote: [\[CITE\]](#) Or just stay away from posting proper OPSEC guides on a website such as this which everybody knows logs your IP into a centralized database to then migrate to the cloud/data-brokers for further enhancement and refinement of your digitally unique identifier and unique digital thumbprint to better understand who you are to provide you with targeted ads based on your geodata

haha. i only joke. Thanks for your contribution here.

Don't worry my brata i am wearing a tinfoil hat and so is my raspberry pi that i destroy after every log in

Just doing my part for the community , hope you learned something !

Tyr - July 15, 2025, 12:28 am

(Jul 15, 2025 12:27 AM)Chorozon Wrote: [\[CITE\]](#) Don't worry my brata i am wearing a tinfoil hat and so is my raspberry pi that i destroy after every log in

Just doing my part for the community , hope you learned something !
atta boy ?

DeathPenalty666 - July 15, 2025, 12:40 am

(Jul 15, 2025 12:27 AM)Chorozon Wrote: [\[CITE\]](#) Don't worry my brata i am wearing a tinfoil hat and so is my raspberry pi that i destroy after every log in

Just doing my part for the community , hope you learned something !
can device like deeper network (dVPN) can be good method?

also any device using mobile network can be traced even if battery is dead, and all you do is logged! there is internet less communication device that reach 12km and moe range, flipper zero who can use mobile network for crypted communication and i would suggest wickr for mobile messaging.

Chorozon - July 15, 2025, 12:49 am

(Jul 15, 2025 12:40 AM)arlalala01 Wrote: [\[CITE\]](#) can device like deeper network (dVPN) can be good method?

also any device using mobile network can be traced even if battery is dead, and all you do is logged! there is internet less communication device that reach 12km and moe range, flipper zero who can use mobile network for crypted communication and i would suggest wickr for mobile messaging.

I can't remember if i referenced in this guide but your right you sim can be pinged if it is in your device so.... remove it ? Don't use a burner phone anywhere near your house 5-12km seems to be the sweet spot to switch cell towers

no no wickr was bought by amazon and is now unsafe i would recommend signal or xmpp using PGP , i am on the fence about threema , some people use session i have not so i won't comment

If your core opsec is good you will have alot less stress about being de-anonymized , think about your fingerprint , rotate devices , identitys and sims and locations

Something unpredictable is hard to predict

I am thinking about a part 2 of this guide to go alot deeper

Lawrencelll - August 29, 2025, 11:28 pm

Awesome thread

Chorozon - August 31, 2025, 1:49 am

(Aug 29, 2025 11:28 PM)Lawrencelll Wrote: [\[CITE\]](#) Awesome thread
Glad your staying safe !

ManiH13 - September 8, 2025, 3:10 am

thanks

Chorozon - September 21, 2025, 8:03 pm

(Sep 8, 2025 03:10 AM)ManiH13 Wrote: [\[CITE\]](#) thanks
Glad you learned something

n9ne_am - November 2, 2025, 7:35 pm

yoooo thanks man actually learned a couple things and am def gonna be upgrading some aspects of my own opsec

DAL-SHA - November 3, 2025, 11:55 pm

Well said and well written guide sir !!

This guide is top of the notch !

Thank you for taking the time and writing this guide sir !

DewGho - November 9, 2025, 6:17 am

Interesting article, I liked it.

But I don't trust some messengers.

Signal is hosted on Amazon servers (I'm skeptical about that).
Tox is a completely vulnerable messenger that can't be updated.
Jabber is good, but only when using PGP or OMEMO encryption (I agree).

I would prefer Simplex to all of these.

And here's a question for the author of the thread: does Mullvad use encryption and VPN protocol hiding?

In other words, will my provider be able to see that I am using one of the VPN protocols?

Thank you.

Chorozone - November 25, 2025, 4:19 am

(Nov 9, 2025 07:17 AM)DewGho Wrote: [\[CITE\]](#) Interesting article, I liked it.

But I don't trust some messengers.

Signal is hosted on Amazon servers (I'm skeptical about that).
Tox is a completely vulnerable messenger that can't be updated.
Jabber is good, but only when using PGP or OMEMO encryption (I agree).

I would prefer Simplex to all of these.

And here's a question for the author of the thread: does Mullvad use encryption and VPN protocol hiding?

In other words, will my provider be able to see that I am using one of the VPN protocols?

Thank you.

Can they break signals encryption is the question though ? I do not think so the so the governments have never been a big fan of it

As i say in the guide alot of these things depend on your baseline opsec

Are you doing crime ? don't do it on your network
Are you running signal or messenger apps on your own phone in your house = broken opsec

Depending on your threat model your opsec baseline should be adjusted its not a one size fits all

ggsf - November 27, 2025, 1:25 pm

Very good thank you

Stanley - December 13, 2025, 7:56 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Lowkey - December 13, 2025, 8:16 am

Good place to start guide.

Horse - December 15, 2025, 5:57 pm

when using clearnet sites never use same identity !

Rick4pex - December 16, 2025, 12:37 pm

You are right, jails in my country are not very fun ?

Thank you for this post, this is an extremely high quality guide ??

johnsbigsnow123 - December 16, 2025, 2:47 pm

Thank you for the guide I'm sure it will be very helpful

Chorozon - December 26, 2025, 2:51 pm

(Dec 16, 2025 03:47 PM)johnsbigsnow123 Wrote: [\[CITE\]](#) Thank you for the guide I'm sure it will be very helpful

Glad you learned something !