

Forum: [Hack Forums](#)

Thread: [List of Secure VPN's - Stop Buying Garbage Sold Here](#)

SUI-3183372 - July 12, 2016, 3:11 am

This is a continuation of my old thread [here](#).

Privacy has become a very dominant interest of mine for a few years now. I've always felt that even people with absolutely nothing to hide deserve to have every option available to them when it comes to their privacy. Everyone deserves to live as private of a life as they desire. Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech.

So....

Every single day I come across discussions about VPN's and what is really secure; And every single day I come across different vendors with a VPS and an OpenVPN installation attempting to offer them security. Maybe it's some hidden goal that a few of you have; to see how many different HF members you can mislead into a false sense of security... but it's incredibly frustrating and mildly infuriating coming into these threads and seeing all the ill advice. It's gotta stop. I've kept a list of strong VPN's I've used and have come to trust, and I'm willing to share it to try and steer some of you away from the bullshit found around here.

- I will not list VPN's that do not offer an anonymous form of payment.
- I am only listing locations I recommend using. Most of these VPN's offer more locations than I have listed, but due to data retention laws and/or invasive governments, those locations may not be entirely secure.
- This topic is not intended for those simply trying to mask their IP's to ban evade, avoid attack, play video games on, etc. Most any VPN is fine for those purposes.
- As most of you already know, a VPN should not be you only line of defense, nor is it likely to find a VPN that is truly logless all the way back to the data center. Do not buy one of these and think that you're safe to say or do anything that you'd like. Additional steps are necessary.
- I am not making these suggestions to aid in the breaking of any laws. I am making these suggestions to help preserve a basic and fundamental human right that is becoming more and more difficult to come by.
- Post here or PM me if you have a reason why one of the below VPN's shouldn't be included.

List made July 20, 2013 | Updated July 12, 2016

This is a work in progress, I'm tired, will add more VPN's later.

***NOTE: NEW RUSSIAN ANTI-TERROR LAWS REQUIRE ALL RUSSIAN INTERNET/SERVER PROVIDERS TO LOG DATA FOR A MINIMUM OF 6-12 MONTHS.**

VPN: [AproVPN](#)

Payment Method: BTC, WMZ

Notable Server Locations: BG, ISL, JP, LV, PA, RO, [RU](#), SE, UA

Price Per Month (Standard): \$12

Price Per Month (Double VPN): \$15

Price Per Month (Quad VPN): \$17

VPN: [AzireVPN](#)
Payment Method: BTC
Notable Server Locations: SE
Price Per Month: \$5.55
Price Per Year: \$50

VPN: [BlackVPN](#)
Payment Method: BTC
Notable Server Locations: CH, EE, LT, LU, NL, [RU](#), UA
Price Per Month: ~\$5.55
Price Per Year: ~\$54.50

VPN: [BolehVPN](#)
Payment Method: BTC, DASH
Notable Server Locations: CH, NL, SE
Price Per Month: \$9
Price Per Year: \$70

VPN: [Double VPN](#)
Payment Method: BTC, PM, WMZ
Notable Server Locations: CH, ES, IT, NL, RO
Price Per Month (Standard): \$25
Price Per Month (Double VPN): \$36
Price Per Month (Multi Double): \$42
Price Per Month (Triple VPN): \$42

VPN: [ExpressVPN](#)
Payment Method: BTC, WMZ
Notable Server Locations: [Way too many for me to list](#)
Price Per Month: \$13
Price Per Year: \$100

VPN: [IPredator](#)
Payment Method: BTC, WMZ, PM, AGC, Cash in mail
Notable Server Locations: SE
Price Per Month: \$8
Price Per Year: Unclear

VPN: [IPVanish](#)
Payment Method: BTC
Notable Server Locations: [Large location list located here](#)
Price Per Month: \$10
Price Per Year: \$78

VPN: [IVPN](#)
Payment Method: BTC, Cash in mail
Notable Server Locations: CH, HK, ISL, NL, RO, SE
Price Per Month: \$15
Price Per 3 Months: \$37

VPN: [Liquid VPN](#)
Payment Method: BTC
Notable Server Locations: CH, NL, RO, SE

Price Per Month: \$7
Price Per Year: \$57

VPN: [Mullvad](#)

Payment Method: BTC, Cash in mail
Notable Server Locations: NL, SE
Price Per Month: 0.0072 BTC - ~\$4.50
Price Per 6 Months: 0.0433 BTC - ~\$27.75

VPN: [Private Internet Access](#)

Payment Method: AGC, BTC, Gift Cards
Notable Server Locations: CH, HK, RO, SE
Price Per Month: \$7
Price Per Year: \$40

VPN: [PrivateVPN](#)

Payment Method: BTC
Notable Server Locations: CH, NL, RO, [RU](#), UA
Price Per Month: \$7.75
Price Per Year: \$73

VPN: [prq.se](#)

Payment Method: BTC
Notable Server Locations: SE
Price Per Month 10 Mbps: 0.03 BTC - ~\$19
Price Per Month 30 Mbps: 0.05 BTC - ~\$32

VPN: [SlickVPN](#)

Payment Method: BTC, Cash in mail
Notable Server Locations: AU, BG, CH, CL, CN, HK, IS, KO, LI, LV, MO, NL, PA, RO, [RU](#), SA, SE, UA
Price Per Month: \$10
Price Per Year: \$48

VPN: [SmartVPN](#)

Payment Method: BTC
Notable Server Locations: IM, NL, [RU](#), UA
Price Per Month: \$6.65
Price Per Year: \$80

VPN: [TorGuard](#)

Payment Method: BTC, LTC, WMZ, many others
Notable Server Locations: BG, CH, CL, CN, EG, ES, HK, IS, IL, LV, MD, NL, RO, [RU](#), others
Price Per Month: \$10
Price Per Year: \$60

VPN: [TrustVPN](#)

Payment Method: BTC, PM, WMZ, Interkassa
Notable Server Locations: AT, CH, CL, EG, ES, IS, IM, LU, MY, NL, NO, RO, SE
Price Per Month: \$15, \$30 for Double VPN
Price Per 6 Months: \$81, \$162 for Double VPN

Know why one of these shouldn't be listed? Tell me.

Rubixa - July 12, 2016, 5:09 am

No doubt dude, these VPN's around here that have 20 dollars for a freaking lifetime.. pfft.

Something isn't right there at all.. Good VPN's cost triple that yearly..

Nice thread, you seem to know what you're on about whenever I see you post.

BITCHLESS - July 12, 2016, 5:13 am

What about nvpn? I hear good review about nvpn

SUI-3183372 - July 12, 2016, 5:24 am

(Jul 12, 2016 05:13 AM)Dramario Wrote: [\[CITE\]](#) What about nvpn? I hear good review about nvpn
Wow, I wasn't aware nVPN was still around. It used to be the most popular VPN on these forums from 2010-2012. Do you know if hellrell still runs it?

Honestly, I don't know enough about it to list it at this time, but hellrell was knowledgeable so I'll reach out to him to ask him some questions if he's still in charge. After five years of running a VPN I'm sure he knows what's up.

Added 10 more VPN's to the list. Will add more later.

Hoodie+ - July 12, 2016, 5:25 am

(Jul 12, 2016 05:13 AM)Dramario Wrote: [\[CITE\]](#) What about nvpn? I hear good review about nvpn
They host their servers on OVH.

SUI-3183372 - July 12, 2016, 5:30 am

(Jul 12, 2016 05:25 AM)Hoodie+ Wrote: [\[CITE\]](#) They host their servers on OVH.
Too many locations to just be using OVH: <https://nvpn.net/order.php?step=1>

However you must choose just 1 location on checkout and you can change locations later. I'm not incredibly fond of that. At the very least, nVPN has to keep a database of which customers are on each location.

Ted™ - July 12, 2016, 5:32 am

Vouch for this
user knows his shit

Hoodie+ - July 12, 2016, 5:34 am

(Jul 12, 2016 05:30 AM)Previously Known As.... Wrote: [\[CITE\]](#) Too many locations to just be using OVH: <https://nvpn.net/order.php?step=1>

However you must choose just 1 location on checkout and you can change locations later. I'm not incredibly fond of that. At the very least, nVPN has to keep a database of which customers are on each location.

That's true.

The nVPn I have is located in France though.

Rubixa - July 12, 2016, 5:34 am

(Jul 12, 2016 05:13 AM)Dramario Wrote: [\[CITE\]](#) What about nvpn? I hear good review about nvpn nVPN are pretty great to be honest, I recommend them a lot to people who ask.

(Jul 12, 2016 05:30 AM)Previously Known As.... Wrote: [\[CITE\]](#) Too many locations to just be using OVH: <https://nvpn.net/order.php?step=1>

However you must choose just 1 location on checkout and you can change locations later. I'm not incredibly fond of that. At the very least, nVPN has to keep a database of which customers are on each location.

Yeah you have the location you choose upon ordering and you have one free server switch, if you wish to switch servers an unlimited amount of times it cost \$10/m

Xen010 - July 12, 2016, 5:35 am

what is about perfect privacy?

SUI-3183372 - July 12, 2016, 5:38 am

(Jul 12, 2016 05:34 AM)Hoodie+ Wrote: [\[CITE\]](#) That's true.

The nVPn I have is located in France though.

OVH is one of the largest, if not the largest, Internet Service Providers in France. They are also the largest web host in the country, and I believe in all of Europe. Would be incredibly likely that most VPN providers using a French location use OVH.

(Jul 12, 2016 05:34 AM)Rubixa Wrote: [\[CITE\]](#) nVPN are pretty great to be honest, I recommend them a lot to people who ask.

Yeah you have the location you choose upon ordering and you have one free server switch, if you wish to switch servers an unlimited amount of times it cost \$10/m

Thanks for the info. I'll see if I can talk to hellrell later (assuming he still runs nVPN).

(Jul 12, 2016 05:35 AM)Xen010 Wrote: [\[CITE\]](#) what is about perfect privacy?

They'll be added to the list later. I'm a bit tired at the moment. They do meet my specifications to be on the list.

Batidas - July 12, 2016, 5:45 am

Useful thread m8, keep it up.

Prawnster - July 12, 2016, 5:49 am

What about cryptostorm? I use it and I have had a pretty great experience so far :D

SUI-3183372 - July 12, 2016, 5:56 am

(Jul 12, 2016 05:49 AM)Mazl Wrote: [\[CITE\]](#) What about cryptostorm? I use it and I have had a pretty great experience so far :D

I do like Cryptostorm, and went to add them to my list. It has been a long time since I used them however, and when I checked their server locations it appeared they removed a majority of their stronger locations. Can you confirm that this list is accurate for their server locations, or do they have more that are not listed? <https://uptime.statuscake.com/?TestID=tZj3HbyKm5>

I wasn't going to list them if their Swiss location is their only strong-ish location left. They are a great company overall though, and I frequently follow their news and updates regarding privacy across the globe.

BITCHLESS - July 12, 2016, 5:56 am

Which vpn is the best if I want crack account via sentry mba?

Lady Killer - July 12, 2016, 5:57 am

Wow thanks for this dude. I saved all of these and will be using this in the future.

(Jul 12, 2016 05:56 AM)Dramario Wrote: [\[CITE\]](#) Which vpn is the best if I want crack account via sentry mba?

Just look for a VPN that has a server that is located close to you and that has unlimited bandwidth!

SUI-3183372 - July 12, 2016, 6:00 am

(Jul 12, 2016 05:56 AM)Dramario Wrote: [\[CITE\]](#) Which vpn is the best if I want crack account via sentry mba?

I don't know anything about Sentry or cracking accounts. It's not something that I want to learn or discuss really. Privacy is what really matters to me. Maybe somebody else can answer your question.

I'm going to sleep. Will post some updates later.

Prawnster - July 12, 2016, 6:20 am

(Jul 12, 2016 05:56 AM)Previously Known As.... Wrote: [\[CITE\]](#) I do like Cryptostorm, and went to add them to my list. It has been a long time since I used them however, and when I checked their server locations it appeared they removed a majority of their stronger locations. Can you confirm that this list is accurate for their server locations, or do they have more that are not listed?

<https://uptime.statuscake.com/?TestID=tZj3HbyKm5>

I wasn't going to list them if their Swiss location is their only strong-ish location left. They are a great company overall though, and I frequently follow their news and updates regarding privacy across the globe.

I am pretty sure that this is the list of servers yea, I dont believe there is more.

They give pretty good privacy from what I am seeing and its not bad speeds, but I am from the UK and the servers over here are pretty good :)

Good list tho, it will help some of the guys that are unsure of what is best to choose!

SUI-3183372 - July 12, 2016, 2:07 pm

Just found out about the new Russian Anti-Terror laws. Their new laws require all VPN servers based in Russia (to be specific, any internet provider in Russia) to keep logs for a minimum of 6 or 12 months (getting conflicting info regarding the length). Private Internet Access has been the first major VPN provider to pull out of Russia now that this is clear.

I will be removing RU locations from my lists. I think it's unlikely that the Russians share their data with other countries, but it still goes against our right to privacy.

th3c0rrupt3d0n3 - July 12, 2016, 2:57 pm

Awesome thread. I can vouch for ZorroVPN and TorGuard, really professional services. I used CryptoStorm too for a month a long time ago, can't complain either.

[censored] is decent too, many locations, good up time, BTC, killswitch other nice features. Another cool one I have used is 24VC, good for Stealths, they don't take BTC though.

And... also have used a \$20 lifetime VPN from HF, it only loads on one location from the 15 advertised?.

(Jul 12, 2016 05:56 AM)Dramario Wrote: [\[CITE\]](#) Which vpn is the best if I want crack account via

sentry mba?

VPN's do not work for that, better get proxies from SSLProxies24.

BITCHLESS - July 12, 2016, 2:59 pm

(Jul 12, 2016 02:57 PM)R??T Wrote: [\[CITE\]](#) Awesome thread. I can vouch for ZorroVPN and TorGuard, really professional services. I used CryptoStorm too for a month a long time ago, can't complain either.

[censored] is decent too, many locations, good up time, BTC, killswitch other nice features. Another cool one I have used is 24VC, good for Stealths, they don't take BTC though.

And... also have used a \$20 lifetime VPN from HF, it only loads on one location from the 15 advertised?.

VPN's do not work for that, better get proxies from SSLProxies24.

VPN + Proxy

I think it's good idea

SUI-3183372 - July 12, 2016, 3:08 pm

(Jul 12, 2016 02:57 PM)R??T Wrote: [\[CITE\]](#) Awesome thread. I can vouch for ZorroVPN and TorGuard, really professional services. I used CryptoStorm too for a month a long time ago, can't complain either.

[censored] is decent too, many locations, good up time, BTC, killswitch other nice features. Another cool one I have used is 24VC, good for Stealths, they don't take BTC though.

And... also have used a \$20 lifetime VPN from HF, it only loads on one location from the 15 advertised?.

VPN's do not work for that, better get proxies from SSLProxies24.

N-o-r-d will be added to the list next update. I've used them before, they were pretty good.

KFC Watermelon - July 12, 2016, 4:11 pm

Most people want a VPN with dedicated port forwarding. Not many realize this, but if you're using a dedicated port on a VPN, you are 100% traceable and there is nothing you (or the VPN owner) can do about it.

Scymo - July 12, 2016, 4:12 pm

(Jul 12, 2016 04:11 PM)KFC Watermelon Wrote: [\[CITE\]](#) Most people want a VPN with dedicated port forwarding. Not many people realize this, but if you're using a dedicated port on a VPN, you are 100% traceable and there is nothing you (or the VPN owner) can do about it.

Can you expand on this?

I'm using Private Internet Access (when not on HF), is this dedicated port forwarding?

KFC Watermelon - July 12, 2016, 4:13 pm

(Jul 12, 2016 04:12 PM)Scymo Wrote: [\[CITE\]](#) Can you expand on this?

I'm using Private Internet Access (when not on HF), is this dedicated port forwarding?

Private Internet Access gives you a unique set of ports every time you connect. They don't offer dedicated port forwarding. By dedicated port forwarding, I mean the same port (or range of ports)

are always open when you connect.

SUI-3183372 - July 12, 2016, 4:49 pm

(Jul 12, 2016 04:11 PM)KFC Watermelon Wrote: [\[CITE\]](#) Most people want a VPN with dedicated port forwarding. Not many realize this, but if you're using a dedicated port on a VPN, you are 100% traceable and there is nothing you (or the VPN owner) can do about it.

That coupled with this, can give users a bad time:

Quote:A newly discovered vulnerability can expose the real IP-addresses of VPN users with relative ease. The issue, which affects all VPN protocols and operating systems, was uncovered by Perfect Privacy who alerted several affected competitors to the threat before making it public.

For the past several years interest in encrypted and anonymous communications has spread to a much wider audience.

VPN providers are particularly popular among BitTorrent users, who by default broadcast their IP-addresses to hundreds of people when downloading a popular file.

The goal of using a VPN is to hide one's ISP IP-address, but a newly discovered vulnerability shows that this is easily bypassed on some providers.

The problem, uncovered by VPN provider Perfect Privacy (PP), is a simple port forwarding trick. If an attacker uses the same VPN as the victim the true IP-address can be exposed by forwarding traffic on a specific port.

The security flaw affects all VPN protocols including OpenVPN and IPSec and applies to all operating systems.

"Affected are VPN providers that offer port forwarding and have no protection against this specific attack," PP notes.

For example, if an attacker activates port forwarding for the default BitTorrent port then a VPN user on the same network will expose his or her real IP-address (in a setting where users share the same IP-address).

The same is true for regular web traffic, but in that case the attacker has to direct the victim to a page that connects to the forwarded port, as Perfect Privacy explains in detail.

The vulnerability affected the setup of various large VPN providers, who were warned last week. This included Private Internet Access (PIA), Ovpn.to and nVPN, who have all fixed the issue before publication.

PIA informs TorrentFreak that their fix was relatively simple and was implemented swiftly after they were notified.

"We implemented firewall rules at the VPN server level to block access to forwarded ports from clients' real IP addresses. The fix was deployed on all our servers within 12 hours of the initial report," PIA's Amir Malik says.

In addition, PIA complimented Perfect Privacy for responsibly disclosing the vulnerability prior to making it public and awarded their competitor with a \$5,000 bounty under its Whitehat Alert Security Program.

Not all VPN providers were tested so it is likely that many others are still vulnerable. Hopefully, these will address the issue in the near future.

Update: PIA's initial solution didn't fix the problem. The company informed its users via email and recommends them to download the latest version of the client.

Asatru Valknut - July 12, 2016, 4:50 pm

I see a total of 3 good ones there.

Tomoko - July 12, 2016, 5:52 pm

Good list you have here, if someone just wants to hide their IP on Skype or something they can get DollarVPN or some other VPN here on HF.

But if you value your privacy, and want a VPN that doesn't keep more than just IP logs(which are useless to the police) I highly recommend PIA and Mullvad.

SUI-3183372 - July 12, 2016, 6:41 pm

(Jul 12, 2016 04:50 PM)Asatru Valknut Wrote: [\[CITE\]](#) I see a total of 3 good ones there.

I expected you to be a multi with some decent knowledge to offer some insight on what you just posted, but after looking at your posting history I was sadly mistaken.

You're wrong.

iNeed Sleep - July 12, 2016, 8:02 pm

(Jul 12, 2016 03:11 AM)Previously Known As.... Wrote: [\[CITE\]](#) VPN: [Double VPN](#)

Payment Method: BTC, PM, WMZ

Notable Server Locations: CH, ES, IT, NL, RO

Price Per Month (Standard): \$25

Price Per Month (Double VPN): \$36

Price Per Month (Multi Double): \$42

Price Per Month (Triple VPN): \$42

AT what point would it be redundant(pointless)? Their largest plan offers to chain you through 4 different VPN server

Altidore - July 12, 2016, 8:17 pm

As many others mentioned nVPN needs to be added to the list.

Some other good ones are:

ovpn.to

airvpn.org

Tokyo - July 12, 2016, 8:22 pm

CryptoStorm is also really nice and anonymous.

SUI-3183372 - July 12, 2016, 8:50 pm

(Jul 12, 2016 08:17 PM)Altidore Wrote: [\[CITE\]](#) As many others mentioned nVPN needs to be added to the list.

Some other good ones are:

ovpn.to
airvpn.org

I'll talk to hellrell later tonight if I can.

(Jul 12, 2016 08:22 PM)Stazzy Wrote: [\[CITE\]](#) CryptoStorm is also really nice and anonymous. I just don't like that they've removed their NL and MD locations. The only location they have that I'd trust anymore is CH. Cryptostorm's team is very advanced though, overall I trust them a lot.

(Jul 12, 2016 08:02 PM)iNeed Sleep Wrote: [\[CITE\]](#) AT what point would it be redundant(pointless)? Their largest plan offers to chain you through 4 different VPN server
It's all a matter of opinion I believe. Do I see the need for a quad vpn? No, not for me. Would I use a double? Sure.

Bambamboom - July 12, 2016, 9:12 pm

I've used nVPN for a long time now, and I love it. Definitely worth the money!

Ambien - July 12, 2016, 9:15 pm

PIA & Mullvad are the only ones I trust.

Alakazam. - July 12, 2016, 10:37 pm

I've NEVER had a problem with nVPN in the couple years i've been using them.

JohnAnonDoe - July 13, 2016, 1:39 am

If you want a full list of VPN's (and their privacy) visit
<https://thatoneprivacysite.net/simple-vpn-comparison-chart/>

7 - July 13, 2016, 1:43 am

Good list, I do use nVPN though and love it. It's a shame not to see it on the list

#Skyline - July 13, 2016, 2:23 am

Dude, you forgot to list proxy.sh

Forc?d - July 22, 2016, 2:19 pm

Did u get in contact with the guy/guys behind nVpn.
My fav for sure, BTC payment with only an E-Mail required.

What would be your recommended best VPN location regarding logging/Privacy laws.

?Criminal - July 22, 2016, 2:30 pm

Zorro logs I shared a zorro login with a guy that did tons of BH activity and the zorro login got terminated and they handed over payment logs and some other data wouldn't trust them at all.

Mi2414 - July 22, 2016, 3:59 pm

PIA is defiantly safe, so is IPVanish.

SUI-3183372 - July 22, 2016, 5:55 pm

(Jul 22, 2016 02:19 PM)Forc?d Wrote: [\[CITE\]](#) Did u get in contact with the guy/guys behind nVpn.
My fav for sure, BTC payment with only an E-Mail required.

What would be your recommended best VPN location regarding logging/Privacy laws.
I never heard back from him, but from what I hear it sounds pretty solid. I don't like that you're confined to 1 location at a time, but that's not the worst.

(Jul 22, 2016 02:30 PM)?Criminal Wrote: [\[CITE\]](#) Zorro logs I shared a zorro login with a guy that did tons of BH activity and the zorro login got terminated and they handed over payment logs and some other data wouldn't trust them at all.

Interesting, I'll remove them to be safe.

Casual - July 22, 2016, 11:02 pm

Huge fan of Mullvad, been using them for years.

Good list!

Powers - July 22, 2016, 11:42 pm

NVPN is also a great vpn, have been using them for a while and haven't had a problem yet.

?yden - July 23, 2016, 12:58 am

I'm pretty sure private internet access offers paypal/credit card for payments. Remember my dad buying it for netflix lmao.

Ympker - July 23, 2016, 1:04 am

Vouching for <https://www.vpnunlimitedapp.com/en> and they even offer lifetime for 100\$ or 39\$ at StackSocial :)

They support nearly any platform and have great servers^^ Very happy so far!

Casual - July 23, 2016, 1:31 am

(Jul 23, 2016 01:04 AM)Ympker Wrote: [\[CITE\]](#) Vouching for <https://www.vpnunlimitedapp.com/en> and they even offer lifetime for 100\$ or 39\$ at StackSocial :)

They support nearly any platform and have great servers^^ Very happy so far!

Jesus dude, you own the site or something?

SUI-3183372 - July 23, 2016, 1:35 am

(Jul 23, 2016 12:58 AM)?yden Wrote: [\[CITE\]](#) I'm pretty sure private internet access offers paypal/credit card for payments. Remember my dad buying it for netflix lmao.
I'm not listing payment methods that may compromise privacy.

JohnAnonDoe - July 23, 2016, 2:55 am

(Jul 23, 2016 01:35 AM)Previously Known As.... Wrote: [\[CITE\]](#) I'm not listing payment methods that may compromise privacy.
PIA are based in USA, they accept PP/CC, BTC or gift cards.

I don't think they keep logs, but where they are located, they shouldn't be trusted.

fortress1999 - July 23, 2016, 4:15 am

Thanks for this mate, really interesting!

SUI-3183372 - July 23, 2016, 4:48 am

(Jul 23, 2016 02:55 AM)JohnAnonDoe Wrote: [\[CITE\]](#) PIA are based in USA, they accept PP/CC, BTC or gift cards.

I don't think they keep logs, but where they are located, they shouldn't be trusted.

To be honest, the US is one of the better locations to host a VPN company. The US has no data retention laws, so it allows secure VPN companies to get away without logging. Other countries, most recently Russia, require internet service providers to now log data for 6-12 months, so Russia is no longer considered to be a secure location when it comes to VPNs. The only downside to the US is the high probability of a raid on your facility. As long as you're not keeping logs though, the raid will reveal nothing. I wouldn't use a US location on my VPN, but I would trust an ethical US company who claim no logs.

JohnAnonDoe - July 23, 2016, 5:01 am

(Jul 23, 2016 04:48 AM)Previously Known As.... Wrote: [\[CITE\]](#) To be honest, the US is one of the better locations to host a VPN company. The US has no data retention laws, so it allows secure VPN companies to get away without logging. Other countries, most recently Russia, require internet service providers to now log data for 6-12 months, so Russia is no longer considered to be a secure location when it comes to VPNs. The only downside to the US is the high probability of a raid on your facility. As long as you're not keeping logs though, the raid will reveal nothing. I wouldn't use a US location on my VPN, but I would trust an ethical US company who claim no logs.

Thanks, I thought US were required to keep logs, but obviously not.

DaUB3R - July 23, 2016, 6:28 am

Nah, OP fuck off. Where was this thread when I was asking for a reliable VPN 3 days ago. ?

I ended up buying nvpn again.

?Criminal - July 23, 2016, 6:32 am

(Jul 23, 2016 12:58 AM)?yden Wrote: [\[CITE\]](#) I'm pretty sure private internet access offers paypal/credit card for payments. Remember my dad buying it for netflix lmao.

PIA's one of my favorites it's pretty fast speeds and you can do practically anything on it and they won't even bat an eye.

Thomaz000 - July 23, 2016, 9:42 am

(Jul 12, 2016 02:07 PM)Previously Known As.... Wrote: [\[CITE\]](#) Just found out about the new Russian Anti-Terror laws. Their new laws require all VPN servers based in Russia (to be specific, any internet provider in Russia) to keep logs for a minimum of 6 or 12 months (getting conflicting info regarding the length). Private Internet Access has been the first major VPN provider to pull out of Russia now that this is clear.

I will be removing RU locations from my lists. I think it's unlikely that the Russians share their data with other countries, but it still goes against our right to privacy.

Would you say that this means VPN providers using Russia locations are LYING to everybody when they say NO logs?

That's what it seems like but maybe some VPN provider can clarify things

And if they are lying about that then how can you trust them.

SUI-3183372 - July 23, 2016, 10:38 am

(Jul 23, 2016 09:42 AM)vonzv Wrote: [\[CITE\]](#) Would you say that this means VPN providers using Russia locations are LYING to everybody when they say NO logs?

That's what it seems like but maybe some VPN provider can clarify things

And if they are lying about that then how can you trust them.

Trustworthy VPN providers have discontinued their Russian locations. Some may actually keep no logs themselves, so they aren't technically lying when they say no logs, but they fail to mention their ISP or DC are now keeping logs, and that's pretty shady. I'd give it a month because it's still a new law, and then see who's claiming what.

SUI-3183372 - July 24, 2016, 3:00 am

(Jul 24, 2016 01:59 AM)Currency Wrote: [\[CITE\]](#) What about this?

<https://hackforums.net/showthread.php?tid=4692270>

If you want you can PM me instead.

It looks decent for a HF VPN, but I doubt he owns his own servers. He is likely using VPS in all of his locations. I personally wouldn't trust a company that doesn't collocate their own servers. You can turn your logs off of your VPN service, but if you're running a VPS you have no idea if the entire dedicated server is being monitored or logged. I ONLY trust companies that use their own hardware.

Rubixa - July 25, 2016, 10:27 pm

Bumping this to the top for obvious reasons.

G1gg1L3s - July 26, 2016, 12:06 am

Stop Buying Garbage Sold Here

That's surely a topic on its own.

henry - August 11, 2016, 11:52 pm

What about vip72 double vpn?

SUI-3183372 - August 12, 2016, 1:46 am

(Aug 11, 2016 11:52 PM)Orang Wrote: [\[CITE\]](#) What about vip72 double vpn?

VIP72 is very good in my opinion, however they're very obviously criminal, their proxy service is based off of compromised machines, so I'm hesitant to add them.

T.NICE - August 12, 2016, 6:09 am

Very nice thread I agree with your list. Prq is made favorite

Cecilia - August 12, 2016, 7:11 am

[https://\[censored\].com/blog/russia-service-update-in-light-of-new-surveillance-law/](https://[censored].com/blog/russia-service-update-in-light-of-new-surveillance-law/)

[censored]'s response to the Russian law.

Eagle 95 - August 13, 2016, 12:43 am

I think this thread should be stuck. As a proven blackhatter, I assume you value your privacy very much. :D

TheChi?f - August 13, 2016, 1:16 am

I am not sure if u have tried this but is CrypticVPN good?

Alprazolam? - August 13, 2016, 7:54 am

Private internet access also allows paypal and has a kill switch. Probably the best hands down.

Meow - August 13, 2016, 10:21 am

What about..

CrypticVPN : <https://hackforums.net/showthread.php?tid=5231265>

143 VPN : <https://hackforums.net/showthread.php?tid=4892146>

Both of them claim that they do not keep logs & both of those services have been on HF for a long time (maybe even when you were active on your 1st account)

Any opinions? I read your thread briefly and couldn't find your reply to those 2 VPN providers.

SIM-82498 - August 13, 2016, 10:24 am

If I'm looking for a dedicated and fresh IP, which of the listed VPNs would suit me best? Fresh as in it hasn't been issued before therefore guaranteeing it is not blacklisted on any website. I used to use www.24vc.com but at \$20/month, I was due to check for better rates.

SUI-3183372 - August 13, 2016, 2:22 pm

(Aug 12, 2016 07:11 AM)LaPanthere Wrote: [\[CITE\]](#)

[https://\[censored\].com/blog/russia-service-update-in-light-of-new-surveillance-law/](https://[censored].com/blog/russia-service-update-in-light-of-new-surveillance-law/)

[censored]'s response to the Russian law.

It's been a bit since I've updated the main OP, but when I do get around to it, N-o-r-d will be there. I respect companies that are proactive in trying to find solutions to the ever growing issue that is personal privacy.

(Aug 13, 2016 01:16 AM)TheChi?f Wrote: [\[CITE\]](#) I am not sure if u have tried this but is CrypticVPN good?

I've been avoiding HF VPN's entirely because there isn't a user here who actually owns their own hardware and collocates it. They just rent VPS' from someone else's hardware, effectively making their claims of privacy an assumption at best. They can not guarantee that there are no logs, they can only guarantee that their VPS on someone else's hardware doesn't keep logs. They have no idea about the dedi its self.

(Aug 13, 2016 07:54 AM)BDSM Wrote: [\[CITE\]](#) Private internet access also allows paypal and has a kill switch. Probably the best hands down.

I don't list PayPal for any of the sites simply because it defeats anonymity.

(Aug 13, 2016 10:21 AM)Meow? Wrote: [\[CITE\]](#) What about..

CrypticVPN : <https://hackforums.net/showthread.php?tid=5231265>

143 VPN : <https://hackforums.net/showthread.php?tid=4892146>

Both of them claim that they do not keep logs & both of those services have been on HF for a long time (maybe even when you were active on your 1st account)

Any opinions? I read your thread briefly and couldn't find your reply to those 2 VPN providers.

143 stores and transmits log in information in plain text (or at the very least is visible to staff (confirmed from a 143 user)), CrypticVPN seems more professional, but read what I wrote above about not owning your own hardware. If I HAD to choose an HF provider, it'd likely be Cryptic, but by choice, I'd never buy a VPN here. I also vaguely remember [RA4W](#) being a fairly knowledgeable user when it comes to VPN's. I don't know much about his service, but again if I HAD to find a VPN on HF, I'd look into his as well.

(Aug 13, 2016 10:24 AM)Dervie Wrote: [\[CITE\]](#) If I'm looking for a dedicated and fresh IP, which of

the listed VPNs would suit me best? Fresh as in it hasn't been issued before therefore guaranteeing it is not blacklisted on any website. I used to use www.24vc.com but at \$20/month, I was due to check for better rates.

Idk much about VPN's that can offer you dedicated and fresh IP's. It throws a lot of anonymity out the window when you use dedicated IPs.

Confound - August 13, 2016, 2:41 pm

This seems like a very useful thread and will surely help many users. Nice work OP.

Mooncake - August 13, 2016, 3:54 pm

Intend to list any residential VPNs capable of bypassing commercial IP blocks and suitable for unbanning gamers ?

SUI-3183372 - August 13, 2016, 4:55 pm

(Aug 13, 2016 03:54 PM)Profitvolt Wrote: [\[CITE\]](#)

Intend to list any residential VPNs capable of bypassing commercial IP blocks and suitable for unbanning gamers ?

Nah, I don't know much about gaming VPN's, just privacy and anonymity.

(Aug 13, 2016 04:01 PM)Yani Wrote: [\[CITE\]](#) This comparison is better:

<https://thatoneprivacysite.net/vpn-comparison-chart/>

(let it load for a while and click show all entries)

Good list. Terrible, shitty, awful website.

Exported to Excel and put online for anyone who wants to view it in a clean manner:

https://docs.google.com/spreadsheets/d/1kKfpAbKMrILTqomZHsbX7cB5hrHZMmgT6yAeH4_j37I/pubhtml

Y?ung Thug - August 13, 2016, 10:39 pm

Nice to see PIA on there, what I use myself.

SIM-3181716 - August 13, 2016, 11:27 pm

I think you should link cryptostorm (<https://cryptostorm.is/>).

SUI-3183372 - August 14, 2016, 1:08 am

(Aug 13, 2016 11:27 PM)Gage. Wrote: [\[CITE\]](#) I think you should link cryptostorm (<https://cryptostorm.is/>).

I love Cryptostorm developers, but their location list has gotten so weak in the recent months that I didn't add them. They deserve a spot though. I guess I'll put them on in my next update.

Meow - August 14, 2016, 1:09 pm

Another one from HF, pretty bold claims and they apparently do not keep logs.

<https://hackforums.net/showthread.php?tid=5355762>

Spoiler ([Click to View](#)) (Jul 29, 2016 01:08 AM)ArtMachine Wrote: [\[CITE\]](#) Thank you. We don't log any of the activities.

Bunch of "vouches" (mostly from Royalty members) saying that VPN is awesome, that it truly doesn't keep logs and all that stuff.

For \$10 lifetime seems too good to be true (no logs, awesome speeds, multiple locations)

Any opinions?

SUI-3183372 - August 14, 2016, 1:33 pm

(Aug 14, 2016 01:09 PM)Meow? Wrote: [\[CITE\]](#) Another one from HF, pretty bold claims and they apparently do not keep logs.

<https://hackforums.net/showthread.php?tid=5355762>

Spoiler ([Click to View](#))

Bunch of "vouches" (mostly from Royalty members) saying that VPN is awesome, that it truly doesn't keep logs and all that stuff.

For \$10 lifetime seems too good to be true (no logs, awesome speeds, multiple locations)

Any opinions?

I mean, they likely do have logs disabled on their configurations, so their claim is technically valid. It's just they're more than likely renting VPS and installing OpenVPN software on it. They have no idea what's being logged on the dedi as a whole. Again, this is why I only trust VPN providers that own their own hardware. For these small HF providers, it's simply not feasible for them to invest that much money into their own hardware. They aren't privacy experts so they're not going to get the following and customer base that comes with being such.

Meow - August 14, 2016, 1:47 pm

(Aug 14, 2016 01:33 PM)Previously Known As.... Wrote: [\[CITE\]](#) I mean, they likely do have logs disabled on their configurations, so their claim is technically valid. It's just they're more than likely renting VPS and installing OpenVPN software on it. They have no idea what's being logged on the dedi as a whole. Again, this is why I only trust VPN providers that own their own hardware. For these small HF providers, it's simply not feasible for them to invest that much money into their own hardware. They aren't privacy experts so they're not going to get the following and customer base that comes with being such.

"We don't log any of the activities."

Yeah that's what I was thinking, THEY don't log the activities but since they are probably renting VPS they are keeping logs (company that they rent VPS from keeps logs). (if that makes any sense)

Thanks for reply anyway

Eagle 95 - August 16, 2016, 12:59 am

Copied from another of your threads but didn't get an answer. ?

Today, what do you recommend to protect your privacy online and offline for an average user?

Intermediate - August 16, 2016, 1:16 am

I've had nothing but good experiences from Private Internet Access, they are really the only ones I trust.

Alesana - August 16, 2016, 1:18 am

I've used a few over the years and PIA has been the one I've stuck with.

SUI-3183372 - August 16, 2016, 4:37 pm

(Aug 16, 2016 12:59 AM)Eagle 95 Wrote: [\[CITE\]](#) Copied from another of your threads but didn't get an answer. ?

Today, what do you recommend to protect your privacy online and offline for an average user?

Sorry, I forgot. I replied on the other thread. It's still a work in progress reply, but there's a start. Very little of it is actually written by me, but compiled elsewhere.

(Aug 13, 2016 01:17 AM)Eagle 95 Wrote: [\[CITE\]](#) Today, what do you recommend to protect your privacy online and offline for an average user?

Sorry for the delay, I saw this question and was gonna put it off for later then forgot about it. There is quite a lot I recommend, but it depends how in depth you want to go. I'm going to list a lot of information. Most of it will be copied from elsewhere, I'll attempt to post sources at the end, however a lot of it is stored as .txt's on my PC and I no longer have the source.

Encryption of data:

I use TrueCrypt full disk encryption for all of my drives and partitions, not just my OS. I've heard [VeraCrypt](#) is a good alternative now that TrueCrypt has reached EOL, but I haven't tried it yet. VeraCrypt is also [receiving an official audit](#) to ensure reliability and security

Key disclosure law - Who is required to hand over the encryption keys to authorities?

Mandatory key disclosure laws require individuals to turn over encryption keys to law enforcement conducting a criminal investigation. How these laws are implemented (who may be legally compelled to assist) vary from nation to nation, but a warrant is generally required. Defenses against key disclosure laws include steganography and encrypting data in a way that provides plausible deniability.

Steganography involves hiding sensitive information (which may be encrypted) inside of ordinary data (for example, encrypting an image file and then hiding it in an audio file). With plausible deniability, data is encrypted in a way that prevents an adversary from being able to prove that the information they are after exists (for example, one password may decrypt benign data and another password, used on the same file, could decrypt sensitive data).

Virtual Private Networks:

I always recommend using a good VPN, even for normal every day browsing.

View my [other thread for my personal VPN suggestions](#). Or view this [large spreadsheet that I put up on Google Docs](#) (note that I did not compile this data, source is at the bottom of the spreadsheet).

And here is a [good guide on making VPNs more secure](#).

Browser Choice and Security:

First things first, I will never recommend using Google Chrome and nothing any of you can say will change my mind on this.

[Firefox](#) is fast, reliable, open source and respects your privacy.

[Tor Browser](#) is your choice if you need an extra layer of anonymity. It's a modified version of Firefox, it comes with pre-installed privacy add-ons, encryption and an advanced proxy.

Browser Fingerprint - Is your browser configuration unique?

When you visit a web page, your browser voluntarily sends information about its configuration, such as available fonts, browser type, and add-ons. If this combination of information is unique, it may be possible to identify and track you without using cookies. EFF created a Tool called [Panopticklick](#) to test your browser to see how unique it is.

WebRTC IP Leak Test - Is your IP address leaking?

WebRTC is a new communication protocol that relies on JavaScript that can leak your actual IP address from behind your VPN. While software like NoScript prevents this, it's probably a good idea to block this protocol directly as well, just to be safe.

For Google Chrome users: There is no known working solution, only a plugin that is easily circumvented. Please use Firefox instead.

For Firefox users: [\(Click to View\)](#)

Code How to disable WebRTC in Firefox?

In short: Set "media.peerconnection.enabled" to "false" in "about:config".

Explained:

Enter "about:config" in the firefox address bar and press enter.

Press the button "I'll be careful, I promise!"

Search for "media.peerconnection.enabled"

Double click the entry, the column "Value" should now be "false"

Done. Do the WebRTC leak test again.

If you want to make sure every single WebRTC related setting is really disabled change these settings:

`media.peerconnection.turn.disable = true`

`media.peerconnection.use_document_iceservers = false`

`media.peerconnection.video.enabled = false`

`media.peerconnection.identity.timeout = 1`

Now you can be 100% sure WebRTC is disabled.

[Test for WebRTC leaks here.](#)

Improve your security with these Firefox add ons

Stop tracking with "Disconnect"

Founded in 2011 by former Google engineers and a consumer-and privacy-rights attorney. The addon is open source and loads the pages you go to 27% faster and stops tracking by 2,000+ third-party sites. It also keeps your searches private.

<https://addons.mozilla.org/firefox/addon/disconnect/>

Block Ads with "uBlock Origin"

An efficient wide-spectrum-blocker that's easy on memory, and yet can load and enforce thousands more filters than other popular blockers out there. It has no monetization strategy and is completely open source. We recommend FireFox but uBlock Origin also works in other browsers such as Safari, Opera, and Chromium. Unlike AdBlock Plus, uBlock does not allow so-called "acceptable ads".

<https://addons.mozilla.org/firefox/addon/ublock-origin/>

Hinder Browser Fingerprinting with "Random Agent Spoofer"

A privacy enhancing firefox addon which aims to hinder browser fingerprinting. It does this by changing the browser/device profile on a timer. Source code: GitHub.

<https://addons.mozilla.org/firefox/addon/random-agent-spoofers/>

Automatically Delete Cookies with "Self-Destructing Cookies"

Automatically removes cookies when they are no longer used by open browser tabs. With the

cookies, lingering sessions, as well as information used to spy on you, will be expunged.

<https://addons.mozilla.org/firefox/addon/self-destructing-cookies/>

Encryption with "HTTPS Everywhere"

A Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. A collaboration between The Tor Project and the Electronic Frontier Foundation.

<https://www.eff.org/https-everywhere>

Block Content Delivery Networks with "Decentraleyes"

Emulates Content Delivery Networks locally by intercepting requests, finding the required resource and injecting it into the environment. This all happens instantaneously, automatically, and no prior configuration is required. Source code: GitHub.

<https://addons.mozilla.org/firefox/addon/decentraleyes/>

Stop cross-site requests with uMatrix

Many websites integrate features which let other websites track you, such as Facebook Like Buttons or Google Analytics. uMatrix gives you control over the requests that websites make to other websites. This gives you greater and more fine grained control over the information that you leak online.

<https://addons.mozilla.org/firefox/addon/umatrix/>

Be in total control with "NoScript Security Suite"

Highly customizable plugin to selectively allow Javascript, Java, and Flash to run only on websites you trust. Not for casual users, it requires technical knowledge to configure.

<https://addons.mozilla.org/firefox/addon/noscript/>

Content control with "Policeman"

This addon has purpose similar to RequestPolicy and NoScript. It's different from the former in that it supports rules based on content type. For example, you can allow images and styles, but not scripts and frames for some sites. It can also be set up to act as a blacklist.

<https://addons.mozilla.org/firefox/addon/policeman/>

This is a collection of privacy related about:config tweaks. We'll show you how to enhance the privacy of your Firefox browser.

Code Preparation:

Enter "about:config" in the firefox address bar and press enter.

Press the button "I'll be careful, I promise!"

Follow the instructions below...

Getting started:

`privacy.trackingprotection.enabled = true`

This is Mozilla's new built in tracking protection.

`geo.enabled = false`

Disables geolocation.

`browser.safebrowsing.enabled = false`

Disable Google Safe Browsing and phishing protection. Security risk, but privacy improvement.

`browser.safebrowsing.malware.enabled = false`

Disable Google Safe Browsing malware checks. Security risk, but privacy improvement.

`dom.event.clipboardevents.enabled = false`

Disable that websites can get notifications if you copy, paste, or cut something from a web

page, and it lets them know which part of the page had been selected.

network.cookie.cookieBehavior = 1

Disable cookies

0 = Accept all cookies by default

1 = Only accept from the originating site (block third party cookies)

2 = Block all cookies by default

network.cookie.lifetimePolicy = 2

cookies are deleted at the end of the session

0 = Accept cookies normally

1 = Prompt for each cookie

2 = Accept for current session only

3 = Accept for N days

browser.cache.offline.enable = false

Disables offline cache.

browser.send_pings = false

The attribute would be useful for letting websites track visitors' clicks.

webgl.disabled = true

WebGL is a potential security risk. Source

dom.battery.enabled = false

Website owners can track the battery status of your device. Source

browser.sessionstore.max_tabs_undo = 0

Even with Firefox set to not remember history, your closed tabs are stored temporarily at Menu
-> History -> Recently Closed Tabs. Read these sources for more information on hardening FireFox:

<https://github.com/pyllyukko/user.js>

http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences

Email

Privacy Conscious Email Providers

[ProtonMail](#)

[CounterMail](#)

[NeoMailbox](#)

Email Clients:

[Mozilla Thunderbird](#) - Mozilla Thunderbird is a free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation. Thunderbird is an email, newsgroup, news feed, and chat (XMPP, IRC, Twitter) client.

[MailPile.is](#) (BETA) - A modern, fast web-mail client with user-friendly encryption and privacy features.

Privacy Email Tools

[gpg4usb](#) - A very easy to use and small portable editor to encrypt and decrypt any text-message or -file. For Windows and Linux.

[Mailvelope](#) - A browser extension that enables the exchange of encrypted emails following the OpenPGP encryption standard.

[Enigmail](#) - A security extension to Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

[TorBirdy](#) - This extension configures Thunderbird to make connections over the Tor anonymity network.

[Email Privacy Tester](#) - This tool will send an Email to your address and perform privacy related tests.

Email Alternatives

Bitmessage

Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need not inherently trust any entities like root certificate authorities. It uses strong authentication which means that the sender of a message cannot be spoofed, and it aims to hide "non-content" data.

<https://bitmessage.org/>

I2P-Bote

I2P-Bote is a fully decentralized and distributed email system. It supports different identities and does not expose email headers. Currently (2015), it is still in beta version and can be accessed via its web application interface or IMAP and SMTP. All bote-mails are transparently end-to-end encrypted and, optionally, signed by the sender's private key.

<http://i2pbote.i2p.us/>

RetroShare

Retroshare creates encrypted connections to your friends. Nobody can spy on you. Retroshare is completely decentralized. This means there are no central servers. It is entirely Open-Source and free. There are no costs, no ads and no Terms of Service.

<http://retroshare.sourceforge.net/>

Privacy Respecting Search Engines

If you are currently using a search engines like Google, Bing or Yahoo you should pick an alternative here.

[DuckDuckGo](#) [Tor Link]

The search engine that doesn't track you. Some of DuckDuckGo's code is free software hosted at GitHub, but the core is proprietary. The company is based in the USA.

[Disconnect Search](#)

Search privately using your favorite search engine: Google, Yahoo, Bing and DuckDuckGo are available for selection. It masks your IP address, cookies, and other personal info.

[MetaGer](#)

A metasearch engine, which is based in Germany. It focuses on protecting the user's privacy. Supported by 24 own crawlers of small scale web search engines.

[ixquick.com](#)

Returns the top ten results from multiple search engines. It uses a "Star System" to rank its results by awarding one star for every result that has been returned from a search engine. Based in the USA and the Netherlands.

Password Managers

If you are currently using a password manager software like 1Password, LastPass, Roboform or iCloud Keychain you should pick an alternative here.

[Master Password - Cross-platform](#)

Master Password is based on an ingenious password generation algorithm that guarantees your passwords can never be lost. Its passwords aren't stored: they are generated on-demand from your name, the site and your master password. No syncing, backups or internet access needed.

[KeePass / KeePassX - Local](#)

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. All passwords in one database, which is locked with one master key or a key file. The databases are encrypted using the best and most secure encryption algorithms currently known: AES and Twofish. See also: KeePassX.

[Encryptr - Cloud Based - \(SpiderOak\)](#)

Encryptr is simple and easy to use. It stores your sensitive data like passwords, credit card data, PINs, or access codes, in the cloud. However, because it was built on the zero knowledge Crypton framework, Encryptr ensures that only the user has the ability to access or read the confidential information.

Self Contained Networks

[I2P Anonymous Network](#)

The Invisible Internet Project (I2P) is a computer network layer that allows applications to send messages to each other pseudonymously and securely. Uses include anonymous Web surfing, chatting, blogging and file transfers. The software that implements this layer is called an I2P router and a computer running I2P is called an I2P node. The software is free and open source and is published under multiple licenses.

[GUnet Framework](#)

GUnet is a free software framework for decentralized, peer-to-peer networking and an official GNU package. The framework offers link encryption, peer discovery, resource allocation, communication over many transports (such as tcp, udp, http, https, wlan and bluetooth) and various basic peer-to-peer algorithms for routing, multicast and network size estimation.

[The Freenet Project](#)

Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship. Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection.

[Tor Project](#)

Provides anonymity to websites and other servers. Servers configured to receive connections only through Tor are called hidden services.

[RetroShare](#)

Open Source cross-platform, Friend-2-Friend and secure decentralised communication platform.

Domain Name System (DNS)

[CloudNS - Service](#)

An Australian based security focused DNS provider. Features: DNSCrypt Support to provide confidentiality and message integrity, complete trust validation of DNSSEC enabled names, namecoin resolution of .bit domain names and no domain manipulation or logging.

[DNSCrypt - Tool](#)

DNSCrypt is a protocol for securing communications between a client and a DNS resolver. The

DNSCrypt protocol uses high-speed high-security elliptic-curve cryptography and is very similar to DNSCurve, but focuses on securing communications between a client and its first-level resolver.

[OpenNIC - Service](#)

OpenNIC is an alternate network information center/alternative DNS root which lists itself as an alternative to ICANN and its registries. Like all alternative root DNS systems, OpenNIC-hosted domains are unreachable to the vast majority of the Internet. Only specific configuration in one's DNS resolver makes these reachable, and very few Internet service providers have this configuration.

[NoTrack](#)

A network-wide DNS server which blocks Tracking sites. Currently works in Debian and Ubuntu.

[Namecoin](#)

A decentralized DNS open source information registration and transfer system based on the Bitcoin cryptocurrency.

Encrypted Cloud Storage Services

If you are currently using a Cloud Storage Services like Dropbox, Google Drive, Microsoft OneDrive or Apple iCloud you should pick an alternative here.

Remember to manually encrypt your files before uploading them to the cloud!

Hosted

[Seafile](#) - 100 GB Storage for \$10/month

Seafile offers 100 GB Storage for \$10/month but also gives you the opportunity to host on your own server. Your data is stored in Germany or with Amazon Web Service in the US for the cloud version. Encrypt files with your own password.

[ownCloud](#) - Choose your hoster

Similar functionally to the widely used Dropbox, with the difference being that ownCloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

[Least Authority S4](#) - For Experts

S4S4 (Simple Secure Storage Service) is Least Authority's verifiably secure off-site backup system for individuals and businesses. 100% client-side encryption and open source transparency. \$25/month for unlimited storage. Servers are hosted with Amazon S3 in the US.

Self Hosted

[Seafile](#)

Seafile is a file hosting software system. Files are stored on a central server and can be synchronized with personal computers and mobile devices via the Seafile client. Files can also be accessed via the server's web interface.

[Pydio](#)

Pydio is open source software that turns instantly any server (on premise, NAS, cloud IaaS or PaaS) into a file sharing platform for your company. It is an alternative to SaaS Boxes and Drives, with more control, safety and privacy, and favorable TCOs.

[Tahoe-LAFS](#)

Tahoe-LAFS is a Free and Open decentralized cloud storage system. It distributes your data across

multiple servers. Even if some of the servers fail or are taken over by an attacker, the entire file store continues to function correctly, preserving your privacy and security.

[ownCloud](#) - Host your own

Similar functionally to the widely used Dropbox, with the difference being that ownCloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

Related Information

[Cryptomator](#) - Free client-side AES encryption for your cloud files. Open source software: No backdoors, no registration.

Text and Video Messaging

Secure your text messages, Instant Messaging and Chat

[Pidgin](#) + [OTR](#) (Windows)

Pidgin is a popular free and open source IM client that lets you chat to users on AIM, Google Talk, MSN, Yahoo and many more. OTR (Off-the-road) is a plugin that combines AES encryption, perfect forward secrecy, and the SHA-1 hash function to ensure strong encryption for IM sessions. As with GnuPG for emails, initial setup is a bit of a pain, but once done operation is seamless (we now have a detailed guide for this).

Tox.im is not a secure solution any longer. There is internal conflict between the devs, a break off with IP being stolen, and some devs claiming the NSA have been pushing bug fixes (open source) with exploits that allow them to monitor things.

[Adium \(OSX\)](#)

Adium is a free and open source messaging client for Mac that also lets you talk to friends on lots of different networks. Even better, Addium comes with OTR support built-in!

[TorChat](#)

[ChatSecure](#)

[SilentCircle](#)

[Surespot](#)

[Jitsi](#)

[Textsecure](#)

[Cryptocat](#)

There's a lot more for me to add, but I'm tired and need to do some stuff, so I'll stop here for now.

notahax0r - August 16, 2016, 5:05 pm

You dont have cryptostorm in the list? What is wrong with you

SUI-3183372 - August 16, 2016, 5:10 pm

(Aug 16, 2016 05:05 PM)notahax0r Wrote: [\[CITE\]](#) You dont have cryptostorm in the list? What is wrong with you

I love Cryptostorm, they're honestly one of my favorites. Just their location list leaves so much to be desired right now. It used to be better.

John F. Kennedy - August 22, 2016, 10:10 pm

Any opinions on www.proxy.sh ?

I had a friend who did some illegal shit on the VPN and he was pretty cocky about it, so I assume it was either good, or he's an idiot.

SUI-3183372 - August 22, 2016, 10:15 pm

(Aug 22, 2016 10:10 PM)John F. Kennedy Wrote: [\[CITE\]](#) Any opinions on www.proxy.sh ?

I had a friend who did some illegal shit on the VPN and he was pretty cocky about it, so I assume it was either good, or he's an idiot.

Proxy.sh is a toss up, it depends how you feel about the following:

<https://torrentfreak.com/proxy-sh-vpn-provider-monitored-traffic-to-catch-hacker-130930/>

Proxy.sh are very transparent with what they do with their servers, which is good, but they will run Wireshark on the network when they deem necessary, which is good and bad, depending on if you trust them to decided what necessary means. Also goes to show that they already have plan ready to log servers quickly and easily. Hopefully they are always transparent when doing so.

Edit:

Apparently they consider these acts to bad enough to warrant the installation of Wireshark on a node:

- Paedophilia;
- Physical supply of materials directly harmful to human beings (drugs, weapons, etc.);
- Activities planning and executing the death of other human beings (assassination, bombing, etc.);
- Identity theft to the extent of committing crimes on the behalf of someone else.

Personally I feel they are overstepping a bit, it's not up to them to police the internet, leave it to LE. But to each their own I suppose.

notahax0r - August 23, 2016, 3:16 am

(Aug 22, 2016 10:10 PM)John F. Kennedy Wrote: [\[CITE\]](#) Any opinions on www.proxy.sh ?

I had a friend who did some illegal shit on the VPN and he was pretty cocky about it, so I assume it was either good, or he's an idiot.

Your friend is an idiot for thinking he is secure from virtual traces only being on a VPN.

Zink - August 24, 2016, 9:13 am

Thanks for the list mate, these were noted and are actually useful. Stopped buying VPN's off here due to lack of stability and privacy.

BorkoSquad - August 24, 2016, 9:55 am

Yeah, I wouldn't recommend buying vpns off of HF. Thanks for this, this list will help a lot of people out.

I'm just curious though, why didn't you list [censored]?

Pittinger - September 24, 2016, 4:19 am

Thanks for this thread.

Unrelated to the original question, but was mentioned later so I'd like to ask, why is LastPass not secure?

The Silenced - September 24, 2016, 4:27 am

Definitely a good list fam. Curious about the first one that offers a double VPN and stuff, that sounds pretty secure. Personally I like PIA, they have always done great in the past..But yeah man much

appreciated on sharing the list!

Lante - September 24, 2016, 5:45 am

(Aug 13, 2016 02:22 PM)Previously Known As.... Wrote: [\[CITE\]](#) It's been a bit since I've updated the main OP, but when I do get around to it, N-o-r-d will be there. I respect companies that are proactive in trying to find solutions to the ever growing issue that is personal privacy.

Wondering as to when we can expect a thread update, as I'm a [censored] customer myself.

sLACKER - September 25, 2016, 7:36 pm

I have been a BIG fan of nVPN for a very long time. I may have only recently joined here on hf bit have been around the net for almost 2 decades.

Cyrus - October 6, 2016, 4:52 pm

Good thread buddy. ?

Messi10 - October 6, 2016, 4:56 pm

nice post, thanks for this list, checking some vpn right now

Rubixa - October 8, 2016, 10:59 pm

Bumping this up, seen alot of people asks about VPN's lately and I love this thread.

SUI-3183372 - October 8, 2016, 11:23 pm

Maybe tomorrow I'll stop being lazy and revise this some more.

Gachi - October 9, 2016, 11:30 am

(Oct 9, 2016 11:25 AM)Fictional Wrote: [\[CITE\]](#) Brother not posting cryptostorm, is he out of his mind? I was literally just about to post this lol

virtualized - October 9, 2016, 11:45 am

This seems like a good thread, I will bookmark it to come back later. :)

SUI-3183372 - October 9, 2016, 12:53 pm

(Oct 9, 2016 11:25 AM)Fictional Wrote: [\[CITE\]](#) Brother not posting cryptostorm, is he out of his mind?

(Oct 9, 2016 11:30 AM)Gachi Wrote: [\[CITE\]](#) I was literally just about to post this lol

I wrote why numerous times in the thread.

I love Cryptostorm. As developers and privacy advocates, they're one of the best. But recently they've cut back the locations they offer on their VPN drastically, so I'm a bit concerned. I still recommend them, but I want to learn more about their reasoning on doing this before re-adding them to my list.

coocochoi - October 11, 2016, 12:39 am

lovely post, this would be helpful. Thanks for the post

memory - December 12, 2016, 2:56 pm

Thank you for the informative and well put together thread. I too am just finding out about the Russia data retention laws, because of this thread. Thank you for the information, I will likely be purchasing a VPN that is listed here on this thread.

Cecilia - December 13, 2016, 2:29 am

You've still not added [censored] to the list, any reason?

hrustovi64 - December 13, 2016, 1:58 pm

Any opinion on [censored]?

SUI-3183372 - December 13, 2016, 2:17 pm

(Dec 13, 2016 02:58 PM)hrustovi64 Wrote: [\[CITE\]](#) Any opinion on [censored]?

They're better than people would assume, as mainstream as they were early on, but I wouldn't put my trust in them fully.

They're based out of Romania and own a lot of their own hardware, but they do rent a lot of it too, which I don't like to see on VPN's that you wish to fully trust.

Their "No Spy Proxy servers" are probably pretty solid though.

SIM-3407314 - December 28, 2016, 10:48 pm

The list doesn't have Cryptostorm in it.... I am disappointed. Very dissapointed. Considering they are one of the only providers to make use of gresec and proper VPN tunnels for the multihop (voodoo) network, a seriously anonymous token-based authentication system, and an admin who is very smart behind a monitor (hands on the keyboard of course).

I can vouch for both IVPN and nVPN like the comments have stated here. Both have errr.. been the holy Jesus and "saved me" lol. But you should do some looking into Cryptostorm on your own. Ask around on the IRC and see what you think.

Edit: saw the comment scrolling back about locations. They have plenty now - check the GitHub for the new config files :)

FractumSeraph - December 28, 2016, 10:51 pm

No love for AirVPN?

They've always been a good friend for me.

<https://airvpn.org/>

(Dec 28, 2016 11:48 PM)CryptoSeb Wrote: [\[CITE\]](#) The list doesn't have Cryptostorm in it... Vouch, Cryptostorm is amazing as far as true anonymity goes.

SUI-3183372 - December 29, 2016, 12:03 am

(Dec 28, 2016 11:48 PM)CryptoSeb Wrote: [\[CITE\]](#) The list doesn't have Cryptostorm in it.... I am disappointed. Very dissapointed. Considering they are one of the only providers to make use of gresec and proper VPN tunnels for the multihop (voodoo) network, a seriously anonymous token-based authentication system, and an admin who is very smart behind a monitor (hands on the keyboard of course).

I can vouch for both IVPN and nVPN like the comments have stated here. Both have errr.. been the holy Jesus and "saved me" lol. But you should do some looking into Cryptostorm on your own. Ask around on the IRC and see what you think.

Edit: saw the comment scrolling back about locations. They have plenty now - check the GitHub for the new config files :)

I haven't had a CryptoStorm account in a bit. I'll check out their GH tomorrow. I do want to make it clear that I love CryptoStorm and the devs over there. They're brilliant.

Also this list is a bit dated at this point, I really need to make some time to review and update it.

I really wish nVPN would respond to my emails. They started as an HF VPN provider so I want to know how they've progressed since leaving this site.

Altidore - December 29, 2016, 8:35 am

(Dec 29, 2016 01:03 AM)Previously Known As.... Wrote: [\[CITE\]](#) I really wish nVPN would respond to my emails. They started as an HF VPN provider so I want to know how they've progressed since leaving this site.

Not sure how you contacted them, hopefully not through HF pm system, i know their not on HF anymore. I'm in contact with the owner from around the way and can forward your message to them, i'm sure it will be replied.

W?lr?? - December 29, 2016, 8:38 am

I think Private Internet Access is one of my favorites because they have shown multiple times in court that they do not keep logs (besides payment data). I'd say it's the best choice.

SIM-3407314 - December 29, 2016, 10:11 am

(Dec 29, 2016 09:38 AM)W?lr?? Wrote: [\[CITE\]](#) I think Private Internet Access is one of my favorites because they have shown multiple times in court that they do not keep logs (besides payment data). I'd say it's the best choice.

They also have a picture of a family riding bicycles together on their homepage and a Twitter handle @buyvpnservice. I would rather not lol.

SUI-3183372 - December 29, 2016, 11:39 am

(Dec 29, 2016 11:11 AM)CryptoSeb Wrote: [\[CITE\]](#) They also have a picture of a family riding bicycles together on their homepage and a Twitter handle @buyvpnservice. I would rather not lol.

You don't use your VPN for family outings in the park? Shame.

Edit: They even have matching helmets. :D

bzr? - December 29, 2016, 1:48 pm

(Dec 29, 2016 12:39 PM)Previously Known As.... Wrote: [\[CITE\]](#) You don't use your VPN for family outings in the park? Shame.

Edit: They even have matching helmets. :D

Marketing done right if you ask me ?

henry - December 29, 2016, 1:53 pm

Looking forward to seeing the list updated

Cz2103 - December 31, 2016, 10:42 am

(Dec 29, 2016 02:53 PM)Orang Wrote: [\[CITE\]](#) Looking forward to seeing the list updated
Any idea how up to date it is currently?

Riddick - December 31, 2016, 2:22 pm

I use Mullvad, they're decent, cheap, easy to use and accept BTC.

SUI-3183372 - December 31, 2016, 3:58 pm

(Dec 31, 2016 11:42 AM)Cz2103 Wrote: [\[CITE\]](#) Any idea how up to date it is currently?

Everything on the list are solutions I still consider to be safe. I'll immediately remove any entry that becomes "unsafe." I just haven't added new entries to the list in some time, and I should do that soon when I find some free time.

FamousHater - December 31, 2016, 4:04 pm

where did u get this info from?

have a feeling i know where but will let u say first

SUI-3183372 - December 31, 2016, 4:06 pm

(Dec 31, 2016 05:04 PM)FamousHater Wrote: [\[CITE\]](#) where did u get this info from?

have a feeling i know where but will let u say first

Combo of TF for information on logging practices and That VPN Guy for more detailed information on practices of the companies.

NoodleBot™ - December 31, 2016, 7:26 pm

Just never assume the VPN is enough. Use some basic precautions to protect yourself further.

SIM-3407314 - December 31, 2016, 8:24 pm

(Dec 31, 2016 08:26 PM)NoodleBot™ Wrote: [\[CITE\]](#) Just never assume the VPN is enough. Use some basic precautions to protect yourself further.

Use Tor. Use Cryptostorm.

It would be a good idea, if you needed to do some work anonymously and have a very small risk factor involved, to use your data connection (tethering your phone) first and skipping your router entirely. Then connect to Tor and route your VPN connection through it. One is probably far more likely to get caught by other means than them providing your VPN provider with a search warrant or forcing them to start logging you with a NSL. Lots of ways they can "find you". I see Twitter skids posting screenshots all the time of them on their ISP and then turning around 4 tweets later and posting links to someone's personal information on SkidPaste. Not that I really want to encourage this type of childish behaviour, but shit. At least grab a free Socks5 son. :/

Revamp - January 7, 2017, 1:18 am

I'm currently using VPN.ac its pretty good.

Cz2103 - January 7, 2017, 10:13 pm

(Dec 31, 2016 09:24 PM)CryptoSeb Wrote: [\[CITE\]](#) Use Tor. Use Cryptostorm.

It would be a good idea, if you needed to do some work anonymously and have a very small risk factor involved, to use your data connection (tethering your phone) first and skipping your router entirely. Then connect to Tor and route your VPN connection through it. One is probably far more likely to get caught by other means than them providing your VPN provider with a search warrant or forcing them to start logging you with a NSL. Lots of ways they can "find you". I see Twitter skids posting screenshots all the time of them on their ISP and then turning around 4 tweets later and posting links to someone's personal information on SkidPaste. Not that I really want to encourage this type of childish behaviour, but shit. At least grab a free Socks5 son. :/

How is cryptostorm different than other VPNs?

SUI-3183372 - January 7, 2017, 11:34 pm

(Jan 7, 2017 11:13 PM)Cz2103 Wrote: [\[CITE\]](#) How is cryptostorm different than other VPNs?

He stated why in an earlier post:

(Dec 28, 2016 11:48 PM)CryptoSeb Wrote: [\[CITE\]](#) The list doesn't have Cryptostorm in it.... I am disappointed. Very dissapointed. Considering they are one of the only providers to make use of gresec and proper VPN tunnels for the multihop (voodoo) network, a seriously anonymous token-based authentication system, and an admin who is very smart behind a monitor (hands on the keyboard of course).

Lante - January 8, 2017, 7:47 am

The "last updated" date in the thread doesn't match the date you last edited it, or was the list itself not altered back then?

I'm also still following this thread and am waiting for the new entries (such as [censored]?) to appear.

SUI-3183372 - January 8, 2017, 2:16 pm

(Jan 8, 2017 08:47 AM)Lante Wrote: [\[CITE\]](#) The "last updated" date in the thread doesn't match the date you last edited it, or was the list itself not altered back then?

I'm also still following this thread and am waiting for the new entries (such as [censored]?) to appear.

Probably just cosmetic update. Tomorrow if I don't forget I'll add content.

?Reath - January 17, 2017, 4:58 am

I'm considering using Private Internet Access in conjunction with OmniRAT, but earlier in the thread I read about some dedicated port forwarding issues and similar things. Can somebody tell me if it's possible and will I have problems with the port forwarding?

IHitNoobs - January 17, 2017, 5:02 am

i use nvpn all the time man and there stuff is amazing and they have no issues changing plus the support is amazing. and they also treat everyone i have had them since 2011 and never had an issue since

KFC Watermelon - January 17, 2017, 9:06 am

(Jan 17, 2017 05:58 AM)?Reath Wrote: [\[CITE\]](#) I'm considering using Private Internet Access in conjunction with OmniRAT, but earlier in the thread I read about some dedicated port forwarding issues and similar things. Can somebody tell me if it's possible and will I have problems with the port forwarding?

Private Internet Access gives you a new set of ports each time you connect, you cannot use it for an application that requires a dedicated port.

?Reath - January 21, 2017, 7:58 am

(Jan 17, 2017 10:06 AM)KFC Watermelon Wrote: [\[CITE\]](#) Private Internet Access gives you a new set of ports each time you connect, you cannot use it for an application that requires a dedicated port.

What about nVPN? Can you recommend me a good VPN with which I'll be able to succeed in my initiative?

Thanks!

Altidore - January 21, 2017, 8:38 am

(Jan 21, 2017 08:58 AM)?Reath Wrote: [\[CITE\]](#) What about nVPN? Can you recommend me a good VPN with which I'll be able to succeed in my initiative?

Thanks!

Like somebody else mentioned PIA has dynamic varying ports, while nvpn has static ports which don't change, makes some things easier, besides nVPN is nice and does what you're looking for.

Viitorul - January 21, 2017, 9:32 am

Thank you man. Very good list!!!

SUI-3183372 - January 21, 2017, 1:44 pm

(Jan 21, 2017 09:38 AM)Altidore Wrote: [\[CITE\]](#) while nvpn has static ports which don't change, makes some things easier, besides nVPN is nice and does what you're looking for.

Is that not concerning to you though? Does that not make you much more identifiable?

In a normal circumstance, if a VPN gets raided and LE are looking for a specific person, there isn't a lot of information to go off. Generally at best they'll get a pool of IP's that connected to the VPN during a specific time frame.

However, I fear that with nVPN these ports that customers set make them a whole lot more identifiable. Not only can LE view the all of the IP's connected during a certain timeframe, but then they should be able to narrow that search down to "just IP's with these specific ports open." With nVPN, at least the last time I used them, you designate what ports you want open in the control panel, meaning these ports are stored in a database somewhere. With access to this database as well as a pool of IP's connected during a specific timeframe, I fear any competent team would be able to narrow their search down to specific IP, or at the very worst, half a dozen IPs.

Someone correct me if I'm wrong, but I've always been under the impression that you want your VPN configured exactly the same way as ever other customer on the VPNs network, so you blend in with everyone. Once you go setting specific options like '5 specific ports you want open' I fear you become shockingly more identifiable.

FintCH - January 25, 2017, 6:35 pm

what about this one ? <https://www.ovpn.se/> !!
they take it seriously

SUI-3183372 - January 26, 2017, 8:57 am

(Jan 25, 2017 07:35 PM)FintCH Wrote: [\[CITE\]](#) what about this one ? <https://www.ovpn.se/> !!
they take it seriously
Yes, ovpn.se is a good provider.

ecc_ecc - February 8, 2017, 2:43 pm

Yo guys, I'm pretty new to this. I want to set up a good VPN. I'm under Linux and was oriented to use ExpressVPN. My question is: have I to pay in BTC or can I use my CC? If I have to pay in BTC how may I do this. I know that this is a Noob question but please help me and lead me doing this.

Thanks.

Edit: another question guys. Using a VPN grants me anonymity when downloading files from mediafire or other file sharing providers?

goondu - April 2, 2017, 6:25 pm

very good information here.

loops77 - April 14, 2017, 11:47 pm

excellent thread here

goondu - April 21, 2017, 5:58 pm

vpn out there that is worth looking

perfectprivacy
bolehvpn
mullvad

Ympker - April 28, 2017, 7:53 am

Personally I am using [censored], Ivacy VPN and VPNunlimitedApp

Black Shadow - April 28, 2017, 3:25 pm

You forgot the best Nvpn thats fast and does not store any data.

I worked for them on customer support for a while.

SUI-3183372 - April 28, 2017, 3:38 pm

(Apr 28, 2017 03:25 PM)Black Shadow Wrote: [\[CITE\]](#) I worked for them on customer support for a while.

Hence why I'll never include them now.

Mirakuru - May 4, 2017, 3:52 am

(Dec 13, 2016 03:29 AM)LaPanthere Wrote: [\[CITE\]](#) You've still not added [censored] to the list, any reason? Could you answer that?

Thanks.

Wings of Redemption - May 5, 2017, 8:41 am

Do any of these support port forwarding?

SUI-3183372 - May 5, 2017, 1:09 pm

(May 5, 2017 08:41 AM)The Rival Wrote: [\[CITE\]](#) Do any of these support port forwarding?

That I don't know. I'm positive some do, I just don't remember which off the top of my head. I don't really support the whole malware/RAT thing anymore, so it wasn't something I was concerned with.

I've been neglecting this list for too long. I have time this afternoon, I may try and update it a bit.

Mirakuru - May 29, 2017, 4:40 pm

(May 5, 2017 08:41 AM)The Rival Wrote: [\[CITE\]](#) Do any of these support port forwarding?

https://www.reddit.com/r/VPNTorrents/comments/3oar5m/list_of_vpns_that_allow_p2p_and_port_forwarding/

summerghost - May 31, 2017, 6:19 am

The above list posted by Mirakuru is legit.

meatyklackers - November 24, 2017, 8:14 am

Went with PIA and I'm happy with it. Really liked the payment options. Nothing like getting secure with a starbucks card. Frappuccino this!

Sh0cka7 - January 22, 2018, 9:03 am

Is this thread going to be updated?

Fear - January 22, 2018, 9:19 am

(Jan 22, 2018 10:03 AM)Sh0cka7 Wrote: [\[CITE\]](#) Is this thread going to be updated?

Just read

https://www.reddit.com/r/VPN/comments/4iho8e/that_one_privacy_guys_guide_to_choosing_the_best/

Cyber Coder - January 22, 2018, 2:14 pm

why isnt nvpn here? i know for a fact that the owner doesnt keep logs and how anonymously he handles his servers

Sh0cka7 - January 22, 2018, 2:35 pm

Thanks for the answer!

Although it was not that kind of information I wanted

I was looking for a compiled list of good VPNs according to BVs standards

But I found what I wanted elsewhere

Fear - January 22, 2018, 5:55 pm

(Jan 22, 2018 03:35 PM)Sh0cka7 Wrote: [\[CITE\]](#) Thanks for the answer!

Although it was not that kind of information I wanted
I was looking for a compiled list of good VPNs according to BVs standards

But I found what I wanted elsewhere
You can find this site on the text

<https://thatoneprivacysite.net/vpn-comparison-chart/>

Sh0cka7 - January 22, 2018, 6:15 pm

(Jan 22, 2018 06:55 PM)Dunkirk Wrote: [\[CITE\]](#) You can find this site on the text

[http s://thatoneprivacysite.net/ vpn-comparison-chart/](http://thatoneprivacysite.net/vpn-comparison-chart/)
I actually didn't see the link!

Thank you very much, that was exactly what I needed!

JahBless - January 23, 2018, 1:45 am

OP you say you only mention VPNs that accept anonymous money transfer but SlickVPN only accepts bitcoin...

And under which email do you register a VPN? Even if you register with a 10minutemail you aren't safe because you haven't got VPN yet, right?

Int Ptr - January 23, 2018, 1:50 am

(Jan 23, 2018 02:45 AM)JahBless Wrote: [\[CITE\]](#) OP you say you only mention VPNs that accept anonymous money transfer but SlickVPN only accepts bitcoin...

And under which email do you register a VPN? Even if you register with a 10minutemail you aren't safe because you haven't got VPN yet, right?

1. Bitcoin is considered an anonymous form of payment, although it does require caution still.
2. Temporary emails should be scrapped after the time period expires, possibly they keep logs, but maybe you can use Tor to register.

Armada - January 23, 2018, 5:30 am

(Jan 23, 2018 02:45 AM)JahBless Wrote: [\[CITE\]](#) OP you say you only mention VPNs that accept anonymous money transfer but SlickVPN only accepts bitcoin...

And under which email do you register a VPN? Even if you register with a 10minutemail you aren't safe because you haven't got VPN yet, right?

You are aware the Black name means OP is banned, right?

RIP Previously Known As.... lol, come home soon .

(Jan 23, 2018 02:50 AM)Int Ptr Wrote: [\[CITE\]](#) 1. Bitcoin is considered an anonymous form of payment, although it does require caution still.

2. Temporary emails should be scrapped after the time period expires, possibly they keep logs, but maybe you can use Tor to register.

^ Pretty much what he said.

Anything and everything takes caution now a days. There really is no such thing as being "Too careful" while online now a days.

Flu0z - January 23, 2018, 8:12 am

(Jul 12, 2016 05:30 AM)Previously Known As.... Wrote: [\[CITE\]](#) Too many locations to just be using OVH: <https://nvpn.net/order.php?step=1>

However you must choose just 1 location on checkout and you can change locations later. I'm not incredibly fond of that. At the very least, nVPN has to keep a database of which customers are on each location.

incorrect

OVH supply many geo-located failover IP's you can use as the IP for the VPN, thus spoofing multiple geo locations while the data center is in fact somewhere else

SUI-3183372 - July 28, 2018, 12:40 pm

After spending a bit of time away from the site ? it seems like I have some updating to do.

I'll entirely update this topic in the next week or so with my personal opinions on the top VPN's, but until then you can use this excellent resource to help you make your decision on VPN's:

<https://thatoneprivacysite.net/vpn-section/>

Geldwolf - July 28, 2018, 12:57 pm

Very nice list dude :-)!

1asdasd1 - November 27, 2018, 11:05 pm

What about ProtonVPN? You should list them too...

SUI-3183372 - November 28, 2018, 12:41 am

(Nov 28, 2018 12:05 AM)1asdasd1 Wrote: [\[CITE\]](#) What about ProtonVPN? You should list them too...

(This post was last modified: 07-22-2016, 04:56 PM by Previously Known As.....)

This list is very out dated, I haven't been keeping up with VPN's lately. However, I'm cautious around ProtonVPN, with their relationship with Tesonet. I'd look elsewhere for a VPN just to be safe, no point taking chances/risks when it comes to privacy.

#Skyline - November 28, 2018, 12:03 pm

(Nov 28, 2018 01:41 AM)Previously Known As.... Wrote: [\[CITE\]](#) (This post was last modified: 07-22-2016, 04:56 PM by Previously Known As.....)

This list is very out dated, I haven't been keeping up with VPN's lately. However, I'm cautious around ProtonVPN, with their relationship with Tesonet. I'd look elsewhere for a VPN just to be safe, no point taking chances/risks when it comes to privacy.

If one day you decide to update this thread.

<https://whoamivpn.com>

We've done abit of work since you last tested it. I'm happy to give you free access anytime tho, just PM me whenever you want.

SUI-3183372 - November 28, 2018, 6:53 pm

(Nov 28, 2018 01:03 PM)#Skyline? Wrote: [\[CITE\]](#) If one day you decide to update this thread.

<https://whoamivpn.com>

We've done abit of work since you last tested it. I'm happy to give you free access anytime tho, just PM me whenever you want.

Thanks, I'll let you know if I ever get back into things. It probably won't be until next summer though.

HackedGh0st - July 29, 2019, 5:16 am

How about Perfect Privacy VPN.....?????

It seems very good to me.....

HackedGh0st - July 29, 2019, 5:17 am

How about Perfect Privacy VPN.....?????

It seems very good to me.....

HackedGh0st - July 29, 2019, 5:18 am

How about Perfect Privacy VPN.....?????

It seems very good to me.....

osk4r - October 6, 2019, 10:11 am

Great, I'm going to use Mullvad thanks for this thread!

fullpain - January 11, 2020, 10:25 pm

Great list, but need some update

Eagle 95 - February 28, 2020, 10:23 am

This is very valuable information to this day.

Winds - February 28, 2020, 10:36 am

Great list. I understand that the list is fairly old but I would avoid Private Internet Access after Kape (AKA [censored]) recently bought them

sway - March 29, 2020, 7:32 pm

Damn this is a good ass selection of vpn's to choose from.

??l?????? - May 6, 2020, 11:25 pm

Wow after so many years still have a valid info :))

Apocryphon - October 12, 2020, 3:45 pm

Thanks for the list. Do you plan to update it anytime soon? :)

What are the best countries for privacy surfing in 2020?

TheCrazyONE - October 13, 2020, 6:25 am

Whos bumping a 2016 thread lol

Avoid expressvpn,pia, and maybe all of them.

Antiquerra - October 15, 2020, 11:52 pm

(Oct 13, 2020 06:25 AM)thecrazy1337 Wrote: [\[CITE\]](#) Whos bumping a 2016 thread lol

Avoid expressvpn,pia, and maybe all of them.

at least add more details on why user should avoid those vpn

\$!uo2H%gE# - October 16, 2020, 2:26 pm

What do you think about ProtonVPN?

I am satisfied with the price, speed and number of servers. The secure core is great too.

.Infinity. - *October 17, 2020, 10:40 am*

when the dude that went to prison recommends vpn services :^)

John Doe - *October 17, 2020, 11:25 am*

What about cryptostorm sir. Very good provider

SUI-3183372 - *October 17, 2020, 11:26 am*

(Oct 17, 2020 11:25 AM)John Doe Wrote: [\[CITE\]](#) What about cryptostorm sir. Very good provider
They're my favorite provider along with Mullvad currently. I just don't have a desire to update my old threads right now.

MOJOKY - *October 22, 2020, 11:38 am*

Thank you for that Useful thread, keep it up.

jull14n - *January 7, 2021, 8:01 am*

Some of them seem untrustable, but I like the list.

Lavaduck - *April 18, 2023, 6:34 am*

very informative, thank you

HerrWinston - *May 31, 2025, 2:33 am*

I really like the list, currently thinking of buying Mullvad thanks to you

?Portishead - *June 11, 2025, 6:59 am*

Is nVpn still good in 2025? I'm looking for something with port forwarding capabilities for command center.