Everything You Need To Know About Private Internet Access (PIA)

You know what? We enjoy rounded little Android-esque characters with a virtual private network (VPN) experience. Whether it's in life or within an app, we think a bit of personality goes a long way.

We were also surprised by these mascots considering Private Internet Access (PIA) is the blandest name you could think of when creating a VPN. The name might be vanilla, but the service is pretty effective, with more than 33,000 servers in 78 countries.

However, is that enough? In this day where privacy matters so much and every VPN service is competing for supremacy, is private internet access and little else enough to entice users?

A year after Mashable's original review, we retested this experience. Private Internet Access continues to be an effective VPN with several improvements. It’s a good, not great, VPN with a few drawbacks that keep it from the very top tier of security options. Pros include improved geo-blocking performance with better access to Netflix and Hulu. The cons include being headquartered in the United States. So far, PIA has not handed over data logs in two court cases and 12 subpoena requests. That’s definitely a good thing, but it could still be compelled to give up user data.

What privacy features does PIA offer?

If you want to access the internet, you need to have an IP address that’s assigned by your internet service provider (ISP). That’s a lot of trust to place in the hands of a giant company. Your ISP could, theoretically, sell your personal data, and it has access to your traffic activity. It may not be monitored or readily available, but chances are you don’t want to have to trust that a company will do the right thing when it comes to your personal data. That’s why you can use a VPN, obscure your IP address, and hide your activity from your ISP.

Upon launching the VPN, we were greeted by a quick tutorial and joined PIA at the month-to-month rate of £9.99 (you get much better deals if you sign up for multiple years). We were given a randomised username and password and was ready to start using the service. You can always create a new, custom password by accessing your account.

The app itself is pretty basic. There’s a slider to toggle your connection and two sections where you can see your server’s location and current IP address. That’s it for the mobile app (it's the same on the iPhone app, which is sort of disappointing since so many VPN services and apps go out of their way to create a full-featured user experience. However, that could be forgiven if PIA delivered with advanced security options. App performance and usability has improved since this review was first published. The interface has been updated, according to PCMag, and mobile apps have also received a nice update, per TechRadar.

There are a lot of security options in PIA, but they're a mixed bag. You can opt to use TCP if you prefer an added sense of security in exchange for speed. There are also multiple options to switch ports for more technical users. Plus you can switch to using small packets for better compatibility with your router.

PIA VPN has a nice feature that lets you block ads and malware while connected. Interestingly, PIA VPN offers a kill switch, but recommends using Android's "Always On VPN" option because it's better integrated. It also automatically enables aggressive IPv6 blocking to prevent any DNS leaks, which might give away your true IP address.

Additionally, you can select your data encryption, authentication, and handshake. These are great features for the tech-savvy user since you're not given a lot of guidance on why you should use AES-128-CBC, the default encryption, over AES-128-GCM, for example.

CBC and GCM are different encryption protocols with the latter being more secure, according to PIA. While GCM is theoretically a more secure encryption protocol, the added security can slow you down, which makes sense since the 128 refers to bits, so 256 means double the bits. It's added security, but leads to a slower experience.

However, all of these features feel like a grab bag of security features. There are a lot of options, and plenty of helpful answers on the PIA website on to how to use them, but some important security features are missing for the Android app. There are no obfuscated servers, which masks VPN activity to look more like regular internet activity. This is an important feature for any user in a country with restrictive internet laws. It's especially important when main competitors such as NordVPN or TunnelBear each offer this feature. If you're in a country that has restricted internet laws and actively monitors for suspected VPN activity, you're likely going to quickly pass on PIA.

The Chromebook extension is similar. While PIA VPN acts as a proxy for Chromebooks, that means no obfuscated servers or ways to change encryption protocols. Instead of a full VPN, which uses an encrypted tunnel to mask your activity before connecting to the VPN's server, a proxy is a basic way to mask your IP address without encryption. However, there were multiple options to limit tracking - such as disabling third-party cookies and blocking malware - or improve privacy, including blocking location access and camera access.

The experience is better on the MacBook Air. We can switch encryption types, add malware protection, activate a kill switch, or request port forwarding.

Despite having somewhat inconsistent experiences between OSes, PIA VPN security features do their job. Testing for domain name service (DNS) leaks revealed no leaks at all. If a website requesting an IP address receives your original IP address and not the VPN's, you have what's called a DNS leak. There are many DNS leak tests online to figure out if you're on a leaky VPN. If the DNS leak test reveals two servers, then you have a leak.

Security features are great, but they can become moot if you can’t trust the VPN company in the first place. PIA VPN says it has a strict “no log” policy - meaning it doesn't keep a log of your internet activity - but you have to believe they are telling the truth. Ua 7 has passed the no-log test twice in courts, but the company behind the VPN is headquartered in the United States and that still leaves a little cause for concern. A year after Mashable's original review, PIA has yet to hand over any data, but the company is still headquartered in the United States.

The United States is a founding member of an intelligence-sharing alliance with up to 14 countries. Known as the Five Eyes alliance, it's a long-standing intelligence-sharing agreement between the U.S., the UK, New Zealand, Australia, and Canada. Any VPN headquartered in on one of these countries may be compelled to give up data it has on its users.

In other words, you should take those no-log claims with a grain of salt.

How does PIA impact connection speed?

U.S. servers for PIA VPN were on par with Mashable's standard service. We noticed some drops in upload speeds, but download speeds were consistently in the 60Mbps range for servers located in New York City, Atlanta, and the Midwest.

We noticed a 10 Mbps drop in my upload speed when we were connected to the Midwest VPN.

Download speeds were better in the UK than France with the latter seeing a close to 20 Mbps drop in speed. Upload speeds were lackluster with both hovering in the teens. It may never be something you notice until you need to send a large file, but it’s something to consider.

We had no speed issues using the Android app. There were negligible 5Mbps drops in download speed, and we never noticed any hiccups or slow-loading images while browsing the web on the default server.

PIA VPN faces another setback with users because it does not bypass Netflix’s strict security measures. Most VPNs are blocked by Netflix ever since the streaming service began actively cracking down on VPN and proxy usage, but this feature would have made PIA VPN a contender even with some of the concerns mentioned previously.

Additionally, PIA VPN does not penetrate China’s “Great Firewall” (although there's a cumbersome workaround(opens in a new tab)). It does support P2P traffic, for those who like to torrent.

Should you consider investing in Private Internet Access?

PIA offers a decent VPN, but that’s about it. There are some good privacy features, but it’s also lacking in obfuscated server support. Speeds are hit-or-miss, but mostly not too bad for a VPN. Speed drops should be minimal for most users who won’t go beyond the default connection. No Netflix is a bummer.

Ultimately, it’s hard to recommend PIA when there are so many VPN options on the market. Sometimes you need more than just internet access that's private.