Stuart Hamby writing sample

Hola: online security that isn't

(297 words)

If you use Hola's VPN services thinking to take advantage of secure, anonymous network connections...you might want to think again. (And if you *aren't* a Hola user, you may want to keep it that way.)

The first thing you need to know is that Hola provides its services through a peer-to-peer (P2P) network. In P2P networking, once connected, other network members use *your* internet connection to browse the internet. That means at the very least that, like it or not, you are donating a portion of your bandwidth to other network users.

Secondly—and a whole lot worse—guest traffic is indistinguishable from your own, legitimate browsing, so there is no way to tell who (some random network member, or *you*) is accessing a website or uploading content. ("Content", which could, for example, be a virus or botware.)

Not that Hola is up-front about the issue of universalized risk. Or the fact that they sell access to their member IPs through a subsidiary (Luminati) for as low as $1.45 per GB with little real vetting. Or the vulnerability that permits network users to install and run programs on *your* computer remotely. (Are you starting to get the picture?)

While Hola claims to have recently issued fixes for some of the above-mentioned threats, other issues are unfortunately inherent to the peer-to-peer structure, and couldn't be redressed even if Hola ripped apart their network and started over. Due to these inherent risks, one group of researchers is advising consumers to uninstall Hola "immediately" and to research other VPN providers.

One legitimately secure, low-cost alternative is ExpressVPN. As a counterpoint to Hola's apparently dangerously flawed P2P design, ExpressVPN creates an SSL secured connection to any website you visit, safeguarding your data and rendering tracking of your metadata much more difficult.