

A Cautionary Privacy Tale for VPN Users

July 19, 2020 - In case you aren't familiar with term VPN, it is an acronym for Virtual Private Network. And a lot of people and businesses use VPN services. That's because they are supposed to protect what you do online from prying eyes. But as we're about to see, that's not always the case.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

VPNs create a secure connection between your computer and another networked computer called a server. That server then connects you to the internet, and allows you to browse freely using the server's IP address. In theory, that makes it impossible for anyone to trace your internet browsing habits back to you.

Additionally, all of the information you transmit between your computer and the server will be encrypted. That means that not even your internet service provider can tell what sites you are visiting or monitor the contents of any messages that you send or receive. In short, VPNs are a fantastic tool for anyone interested in maintaining their privacy or keeping their data secure.

In addition to the privacy aspects, VPNs also serve as a tool to circumvent government restrictions on the websites that internet users can visit. That isn't necessarily something that impacts people in the United States too much, but if you live in communist China, you can't even conduct a search on the Tiananmen Square massacre and be connected to information about it. But VPN users don't have that issue.

As with anything, technology doesn't always function the way that you want it to. And VPNs are no exception. HackRead is reporting that a Hong Kong based VPN provider called UFO VPN has experienced a breach that leaked 20 million user logs. This is a company that claims it doesn't keep user logs. In theory, those logs now have the potential to be used to track down UFO VPN's customers and expose what they have been doing online.

The timing of this couldn't be much worse. The Chinese Communist Party just put a new security law into effect in Hong Kong that allows the Chinese government to circumvent Hong Kong laws and crack down on free speech and freedom of assembly. Anyone who has been using the internet to organize protests in Hong Kong against the Chinese government faces potential extradition to China and a potential sentence of life in prison.

There are also some lessons to come out of this. First, if you are going to use a VPN, you might want to do a little research first. How good is their security? Have they ever been breached? How big is their customer base? Where are

their servers located? And of course, what information is actually contained in their log files.

Second, VPN users should seriously consider using services that are not located in their own countryâ€¦ Hong Kong has actually been a part of China now since the late 1990's. That won't guarantee you that your data won't be exposed, but it will make it more difficult for your own government to get their hands on any log files still in the possession of the service you are using.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS