ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (105-106), Month: October - December 2019, Available at: www.researchpublish.com

VPNs: Safe or Unsafe?

Sameer Z. Eskander

Saudi Aramco

Abstract: **The idea of Virtual Private Networks (VPN) to encrypt data to secure the public internet connection to prevent hacking attacks. In the context of the online privacy, the safest VPNs provide their users with the possibility of being protected and transparent in terms of the corresponding privacy policies, elimination the data browsing history and the log information. Securing the data dependents on the VPN provider which requires latest encryption technology and money to maintain the servers. Keep in mind not all pay VPN services are legitimate and It is important to be careful about who you choose the VPN service provider.**

Keywords: **Virtual Private Networks (VPN), public internet connection, hacking attacks, online privacy.**

1. VPNS: SAFE OR UNSAFE?

The first issue to be considered within the framework of this paper pertains to the representation of the core aspects, pertaining to the functioning of the VPN and the core underlying purposes of its use. As it is stated by the experts, VPNs are created for securing the public internet connection of an individual via the means of encoding one's data and protecting the online activity from ISP, cybercriminals and the providers of the internet services. In the context of the online privacy, the safest VPNs provide their users with the possibility of being protected and transparent in terms of the corresponding privacy policies, elimination the data, about the browsing history and the log information.

In order to understand the core principles of VPN functioning and therefore, the advantages/disadvantages of its use, it is critically important to understand the way, the internet connection works without it. After the address of the web site is typed into the browser, the router gets the information from the ISP that the particular device makes attempts for forwarding the internet traffic to the specific web site.

In addition, the unique number (entitled as Internet Protocol (IP) address) is assigned to the router and devices, connected to it. It is essential to note that there is a set of advertisement networks, websites and platforms, such as Facebook and Google, which use the IP address of an individual for tracing the location, personal data collection of its assessment and evaluation within the frameworks of the corresponding marketing investigations.

When an individual uses the VPN software, the servers of the VPN provider are connected by the device. The internet traffic of the user, in such a case, passes through the internet connection of the VPN. It means that the private information of the user is masked from one's ISP and the websites. Therefore, the web sites are not provided with access to the individual's log data.

The web traffic of different users is mixed by the VPN servers, and therefore, the IP of the particular user matches the corresponding one from the VPN server. Such steps create a set of complications for the web sites and platforms for data collection about the user and monitoring of one's location (Pricop and Stamatescu, 2016).

As it is claimed by the experts, virtual private networks (VPN) represent an effective solution in the context of internet privacy. In the vast majority of cases, the major motivation for using the VPN implies safeguarding in contradiction of cyber snooping. On the other hand, such software may be used by the attackers because they can mask their location online identity to access the blocked websites.

The next issue to be considered in the scope of this paper is the brief representation of the factors, which are sufficient for ensuring the safety of the VPN. It is essential to note that not the same features are inherent to different VPNs, and therefore, each of the existing VPN products has its advantages and disadvantages. Therefore, among the major steps, which are to be undertaken by the user, is to choose the proper VPN, which has the capacity for satisfaction the user's needs, as well as taking into account the price tag.

In the case when no user fees are charged by the VPN provider, the user may pay for the maintenance costs via the advertising or collecting the personal data/opinions and selling them to third parties. In simple terms, it means that while making a choice for the proper VPN, an individual or the management of the enterprise may either prefer to see some advertisement or to pay for one's online privacy. The average cost for the VPN software ranges from 3 to 10 USD monthly. Also, there is a possibility of getting the annual pricing from some providers at a discount.

Among the set of the additional must-have features, which are to be taken into account while preferring the VPN provider, it is possible to outline the following: ensuring the fact that the truly-safe and secure VPN is used. Therefore the set of factors is to be taken into account. First of all, there should not be leaks in the IP addresses; it means that the IP address of the user should be either hidden or disguised as well as other users are to be blocked by the VPN in their attempts of tracing the online activities.

The second issue pertains to the option of "no-logs", which means that no log information is collected by the VPN, as well as there is no option for transmitting the personal data through the network. In simple terms, it means that the provider does not save the personal data of the user when one goes online. Also, no information about the downloads or the browsing history is saved there. Such an approach ensures that the online privacy of an individual and one's anonymity are protected from all other users and the VPN provider, in particular.

The third issue pertains to the 'kill switch' availability, which may be interpreted in the following manner: in the case when there is a drop in the VP connection, the internet access of the user is downgraded to the form of the regular connection. The major role of the VPN kill switch, in this context, is the following: the preselected programs are automatically killed by the switch in the case of connection instability and therefore, the probability of data leaking (from the in the sensitive programs) is minimized in such a case.

The fourth issue to be taken into account while choosing the VPN provider is the multifactor authentication option; such an approach toward security protection is aimed at prompting the users for proving their identity several ways before joining the program (the VPN account). The core purpose of this security measure implies ensuring the fact that only preferred users may access the VPN account of a particular user; in addition, the risk of hacking the account is minimized in such a manner (Bjarnason, 2019).

To conclude, it is possible to make a statement that in the case of preferring the secure VPN service, the individual user or the owner may protect their online information safety, and security. In addition, VPN has a potential for defending the online identity of the user as well as open the set of areas in the World Wide Web, which may be closed for a particular region due to either objective or subjective reasons.

REFERENCES

[1] Bjarnason, S. (2019) *Your Safety and Privacy Online: The CIA and NSA*. InfoSecHelp LLC

[2] Pricop, E. and Stamatescu, G. (2016) *Recent Advances in Systems Safety and Security*. Springer