Research Paper

Do VPNs Work for Mobile Protection

Kevin Murphy

Course Number – 150G

Professor Weather

6/19/2022

Introduction

Technology is constantly advancing and improving our ability to complete tasks with higher efficiency and speed. This speed and efficiency however can act as a double edge sword as in the wrong hands it can lead to criminal behavior and cyber-attacks. The field of cyber security is constantly having to evolve with the times as new vulnerabilities and exploits are being abused. One area in particular is the use of mobile devices. Practically everyone has some sort of smart phone with their private information sitting on that device. Cyber criminals are taking of advantage of that and have ramped up efforts to create more dangerous mobile malware. With that in mind the rise of VPNs has also come to light as you see an increase in advertising and public use. However, that raises the question, do VPNs provide us with enough protection when it comes to mobile device security?

Background

The objective of this paper is to determine the pros and cons of VPNs in terms of their ability to protect our mobile devices. Mobile malware is on the rise, and it is important that people learn if VPNs are truly the solution or just a temporary fix to a growing problem. I will use a mixture of educational websites and peer reviewed articles to determine if VPNs are in fact the best option. VPNs were accessed fifteen years ago originating from virtual Circuits services, or VCs, for businesses to create secure long-distance communication (Kaur & Sharma, 2020).

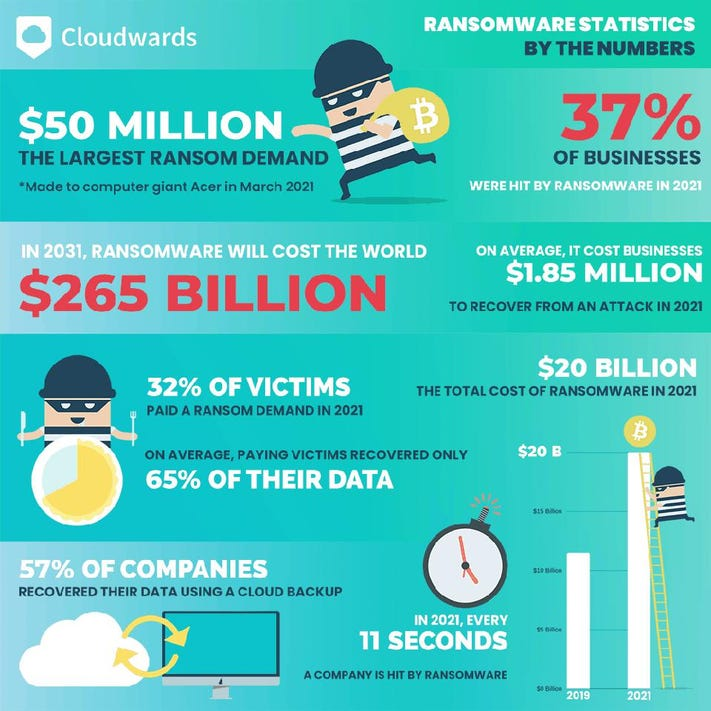
The Pandemic has caused companies to shift to a stay-at-home method causing more cyber-attacks on employees. An article by Partida (2021), cited that 46% of employees downloaded a malicious app and 97% of organizations dealt with mobile threats and attacks in 2020. Cyber Security spending is set to reach $133.7 billion by the end of 2022. The total cost in data breaches estimated around $6 trillion in 2021 (Thakur & Pathan, pg57). 

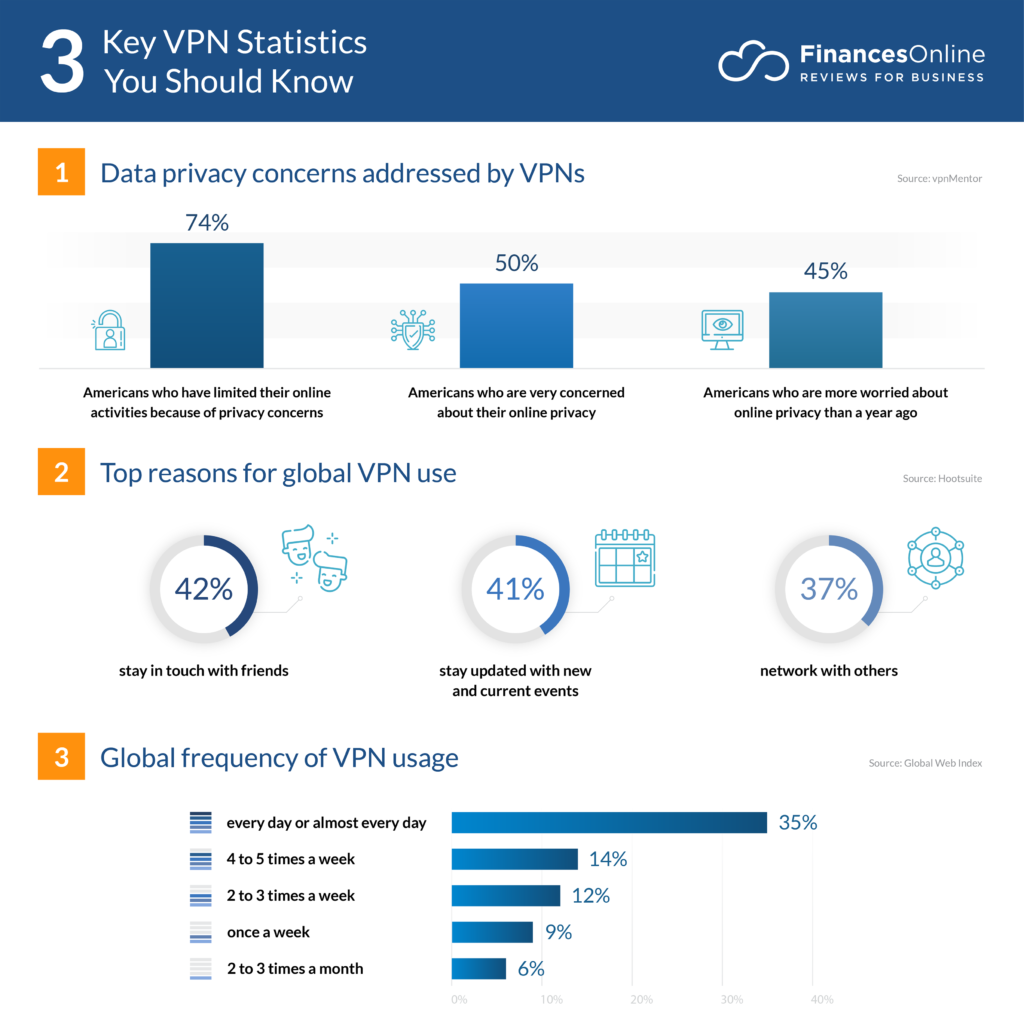
Image from Forbes illustrating the effects of cyber-attacks on companies, claiming that cyber criminals are capable of penetrating 93% (2022) of company networks. 

Image from finace.com (2022) provides context behind the sudden increase in VPN usage rate, mainly revolving around privacy and online security concerns.

What are VPNs

A virtual private network, better known as a VPN, gives you online privacy and anonymity by creating a private network from a public internet connection. The goal of a VPN is to mask the Internet Protocol (IP) address of users, so your actions online are pretty much untraceable. According to Norton, a company that provides VPN services, the most important part of the service is to establish a secure and encrypted connection to ensure greater privacy. VPNs accomplish this by creating

“a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you’re in another place. This benefit allows online freedom, or the ability to access your favorite apps and websites while on the go” (Symanovich, 2022).

VPNs provide the use of data encryption making it difficult to trace back to the original user. VPNs are capable of hiding browser history, IP addresses, location, devices, and other web activity. Most VPN security protocols include point-to-point tunneling (PPTP), Internet Protocol Security (IPSec), Layer 2 Tunnelling Protocol (L2TP), and or Secure Sockets Layer (SSL) and Transport Layer Security (TLS) (Kaur & Sharma, 2020). The overall purpose of VPNs is to provide a better means of online security especially while on the go.

Rise of Mobile Malware

Smart devices are growing in popularity across all devices. These advancements have allowed people to gain access to countless information and services all in the palm of their hands. These mobile devices have become a crucial part of everyday lives both for work and pleasure. This dependency has come with its fair share of security issues, in part due to varying operating systems. The Android OS. for example, has become one of the main targets for mobile malware due to its commitment to open-source code. Open source allows app developer to freely design and install software without the need of paying a license. Although this creates enormous popularity among users and developers it comes with some serious consequences. An article written by authors Qamar, Karim, and Chang (2019), “Mobile malware attacks: Review, taxonomy & future directions”, cited that

“8,225 new malware sample targeted the Android operating system and 744,065 malware are counted during the Q4 in 2017. In addition, malicious applications used evasion techniques to hide as a normal app and detection of these malware is really a challenging task. Recently, 700,000 applications are founded that have malicious content and violate the google play store security policy”.

The major concern stems from the fact that smart phones like Android lack sufficient security measures. This leaves them open to malware attacks such as worms, trojans, and viruses as the smart device is mostly incapable of differentiating a normal application and malware threats. The article (Qamar, Karim, and Chang, 2019) would continue to explain how an infected device can cause severe harmful activities such as locking the phone partially or entirely to make it unusable. Other attacks would cause programs to steal sensitive information, infect contacts, and generate unwanted purchases. These types of attacks are a serious issue causing major financial damage to users and companies across the globe. These devices are also capable of spreading this malware across multiple smart devices in a home making it more difficult to combat data breaches.

Advantages of VPNs

The most important advantage of VPNs comes from its ability encrypt and secure networks. Hackers are using a variety of methods to attack and intercept the sensitive information of users. Using that information, they can attempt to impersonate you, gaining access to bank accounts, credit card information, and more. With a VPN, however, you can utilize high-level security like the 256-bit encryption, which makes all your communications online look like random characters to anyone who tries to intercept them (Norton, 2022). Being able to implement this type of security is beneficial for businesses, especially those who travel. VPNs can secure any network, so users can connect to public networks and ensure that they are secure.

Another advantage of VPNs is the ability to disguise your location and gain access geological freedom, eliminating certain restrictions. Many entertainment sites, like streaming services or certain sports, have varied content depending on the region. Using a VPN, you can make your connection appear in a different region allowing users to gain access to that content that may have been locked previously. Users will be able to enjoy entertainment services, while also applying another layer of security by masking their location.

VPNs are also very easy to use and implement on several devices, at a cost-effective rate. Companies, such as Norton, provide user friendly applications that make securing networks quick and simple. They also provide a means to connect multiple devices to a VPN. According to Kaur & Sharma (2020), VPNs are providing the services comparable to an entire IT support staff. They provide upkeep, performance checks, and server security all for a lower service fee. These services are scalable, so users can apply this level of protection to multiple devices. This is crucial in business environment when you have multiple sensitive devices all connecting to multiple networks.

Disadvantages of VPNs

Although VPNs come with many benefits, they also come with their fair share of complications and issues. One of the major problems that stem form VPN use is the fact that users are at the mercy of third-party protection. Meaning if someone were to hack into one of the companies that provides your VPN, they could gain access to your information that way and you would have no idea. According to an article “Common Vulnerabilities Exposed in VPN” by Bansode and Girdhar (2021), there are a total of 479 known VPN vulnerabilities, in which the top 28 were discovered in 2020. Covid has forced many companies to work from home, resulting in a major uptick in VPN usage. This dependency has come at a cost because now cyber criminals are beginning to find more and more vulnerabilities. Many of these vulnerabilities have been identified due to improper maintenance. VPNs running on older firmware are being exploited due to obsolete software and as a result we are beginning to see VPN hacking occur. Cyber threats like man-in-the-middle attacks, end-to-end attacks or possibly VPN hijacking are creating serious issues for many companies. This rise in attacks has created mistrust from users and a startling grey area as to who should take responsibility, creating even more financial issues. It is crucial that customers and or businesses do the proper research before selecting a VPN service provider. There are numerous companies that have made false claims and promises about their security measures deceiving clients. Android users are some of the primary targets when it comes to fake VPN providers.

Another area of concern when working with VPNs is the speed. VPN services are notorious for reducing internet speeds due to all the processing power required to encrypt the data. This can be especially frustrating for users paying for premium Wi-Fi. There is also the possibility of a VPN dropping its connection altogether (Mason, 2017). This could be problematic if operating with sensitive information on a public network, as once you drop connection with a VPN your information is back online for all to see.

Do VPNs work

So, do VPNs work? I believe that answer is yes. Ultimately the pros outweigh the cons in this situation. The pandemic has created issues for companies trying to stay open and VPNs have made the work at home model possible. VPNs provide a much-needed level of security in order to ensure that users can freely browse the internet and know that their information will be secured. VPNs allow users to mask their location and IP address, making it difficult for potential threats to access sensitive information. Businesses that rely on employees traveling across country or even across the globe can feel better knowing that VPNs will be capable of protecting their devices and give employees access to company systems.

However, a major caveat to this is the type of VPN provider you select. Tech radar (2022) claims that the top three VPNs as of 2022 are ExpressVPN, NordVPN, and Surfshark. Each provide excellent security services and their own special procedures that make them stand above the rest. Nord VPN for example provides extra features like ad block, tracker block, and even blocking malicious websites. Android users especially, need to be wary of the type of VPN they chose to download as there are many fake providers on the app store (Bansode & Girdhar 2021).

Conclusion

VPNs aren’t perfect, but as of right now they are the best solution available, and they will only improve as we continue to advance technologically. Devices are getting faster and more efficient at connecting with one another, which is why protecting our information must become a priority. The rise of malware attacks on mobile devices has become a problem in our everyday lives and we must take a proactive approach in attempting to deal with it. The use of VPNs will play a major role in stopping these attacks and ensuring that our devices remain protected regardless of the virtual environment we might find ourselves. VPNs provide crucial security protocols by encrypting our data, masking our location, providing ad block, and blocking malicious websites. Mobile users and companies, big or small, looking to secure their mobile devices and protect from identity theft will find VPNs are the only real solution.

Citations

* Anthony, J. (2022, January 14). A new version of this article, featuring the latest data and statistics, is available. Check out our report on. Financesonline.Com. <https://financesonline.com/30-key-vpn-statistics-2019-analysis-of-trends-data-and-market-share/>
* Bansode, R., & Girdhar, A. (2021). Common Vulnerabilities Exposed in VPN – A Survey. Journal of Physics: Conference Series, 1714(1), 012045. <https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045/pdf>
* Brooks, C. (2022, January 24). Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. Forbes. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=39b2f03f6b61
* Kaur, C., &amp; Sharma, Y. K. (2020, March 6). The vital role of VPN in making secure connection over internet world. ResearchGate. Retrieved May 23, 2022, from <https://www.researchgate.net/publication/340336829_The_vital_role_of_VPN_in_making_secure_connection_over_internet_world>
* Mason, J. (2017, May 8). ISP Law and the Pros and Cons of VPN Usage. EDUCAUSE. <https://er.educause.edu/blogs/2017/5/isp-law-and-the-pros-and-cons-of-vpn-usage>
* Palmer, D. (2022, March 9). *Smartphone malware is on the rise, here's what to watch out for*. ZDNet. Retrieved May 25, 2022, from <https://www.zdnet.com/article/smartphone-malware-is-on-the-rise-heres-what-to-watch-out-for/>
* Partida, D. (2021, August 11). Mobile Malware: Threats and Solutions. eSecurityPlanet. <https://www.esecurityplanet.com/mobile/mobile-malware-threats-and-solutions/#:%7E:text=Mobile%20malware%20statistics&text=Check%20Point%20published%20mobile%20security,that%20used%20various%20attack%20vectors>.
* Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, 887-909.
* Symanovich, S. (2022, February 24). *What is a VPN?* Norton. Retrieved May 22, 2022, from <https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html>
* Thakur, K., & Pathan, A. K. (2021). Securing Mobile Devices and Technology (1st ed.). CRC Press.
* Williams, M. (2022, June 1). The best VPN service 2022. TechRadar. <https://www.techradar.com/vpn/best-vpn>