Exposure of Privacy during day-to-day device usage

The effects of the internet on society cannot be understated. Massive leaps have been made to its structure, interconnectedness, and usage. However, due to the way it works – transmission towers, undersea cables, signals sent to and from devices for Wi-Fi – there is a certain assumption that people make. Namely, since these signals, wires, and cables are generally taken for granted, people tend to believe that the information sent along these mediums is safe. The idea that “it could never happen to me” causes laxity for their digital privacy and protection – and yet, no one seems to care. A lock doesn’t give a house door total protection; it only makes it harder to break into. There will always be other ways to access information, not from targeted attacks, or widespread data leaks. There will always be signals.

1. Personal Usage

I use my phone and laptop every day for different purposes, whether it be browsing the internet for fun, talking to friends, or looking up things for a project. In all cases, the internet is paramount to these activities. If I lacked an internet connection, there would be several things I could not do, including attending school activities. However, due to how much more I use it, I will be using my phone for comparison.

My phone, a Samsung Galaxy A70, runs Android version 11. I use Firefox as my main browser, with Google as my main search engine. I have a habit of using Firefox’s Private Browsing feature when doing research instead of the normal search, to avoid cluttering up my search history and main page. When I go out, I begin using my mobile data with ProtonVPN, a free VPN service, and when connected to a public or unconnected/untrusted Wi-Fi network, my phone automatically turns on its “Secure Wi-Fi” service, which aims to protect my data. [1]

2. VPNs and IP addresses

I occasionally use a VPN to mask my phone's IP address when browsing the internet. This has a benefit of protecting me online in the case that someone somehow manages to retrieve my IP address but has a downside of being rather slow and draining on my phone's battery. Additionally, VPNs have the potential (but not requirement) to peek at and store the user's data, potentially resulting in a privacy breach.

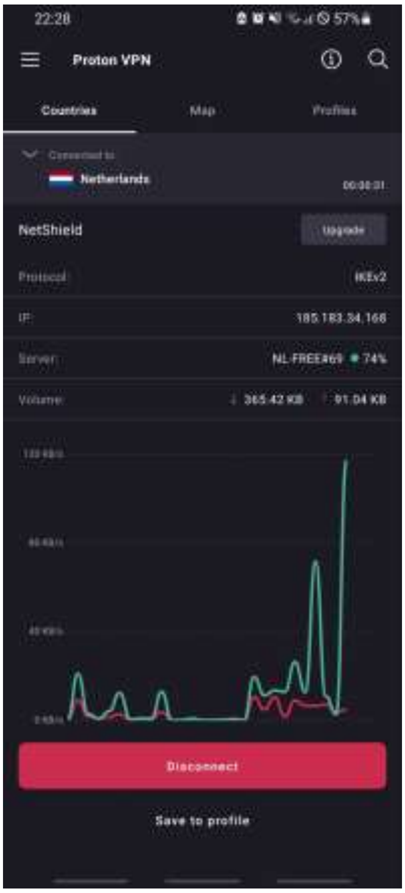
A VPN is a service that grants the user safe and secure access to the internet by encrypting the data sent over the internet and hiding your IP address. [2] This works by creating a “tunnel” through which networks share data through public networks. The data sent is usually encrypted, which aids VPNs in protection, although this isn’t strictly necessary for a VPN to function. VPNs have a variety of uses due to how they mask the user’s IP address, such as bypassing country-restricted content.

Clearly, VPNs are very useful. However, maintaining a service like ProtonVPN doesn't come without costs. Though it is free, it comes with an optional paid subscription service that offers faster speeds and more options. [3] While there are many paid VPN services (such as NordVPN or ExpressVPN), there are several free ones. Why would someone want to pay for a VPN when they could just use a free one?

There are several reasons. A paid service can sometimes appear more trustworthy than a free one, especially when it comes from a name one may have heard before. Plus, paid software is typically better built than free software, because the developers of the app are getting paid to do more. But not everyone wants to pay yet another subscription just to protect their data. And besides, they're careful enough on the internet, aren't they? Why use a VPN at all?

This line of thinking, though faulty, is not without its merits. Since VPNs tunnel user traffic, they at some point need to process this data. What's to stop the company from simply keeping it to sell to advertising companies? For a lot of free services, the product is the user and their data. Even if their app is chock-full of ads, since they have access to your data, they can sell it.

Paid VPN software isn't without fault, either. In early 2018, NordVPN suffered a data breach when one of its servers was accessed without authorization, resulting in a leak of one of the company's expired Transport Layer Security (TLS) keys. [4] The company downplays the event and blames it on their server providers, but such an event happening is still troubling. A TLS key is used to verify that a site is owned by NordVPN. If the key wasn't expired, the breacher could have set up a fake site and exposed thousands of unwilling users to viruses and other malware.



Connected to
Netherlands 00:00:31

NetShield Upgrade

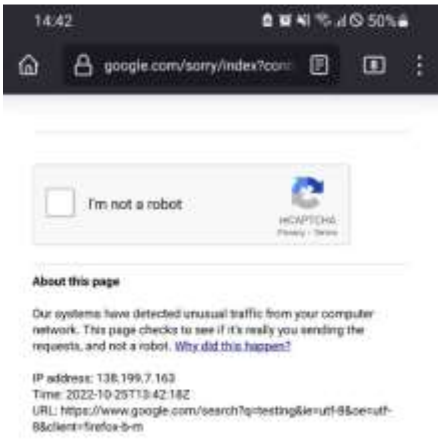
Protocol: IKEv2

IP: 185.183.34.168

Server: NL-FREE#69 74%

Volume: 365.42 KB 91.04 KB

Figure 1: A screenshot of ProtonVPN's mobile user interface



□ I'm not a robot

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 138.199.7.163
Time: 2022-10-25T13:42:18Z
URL: https://www.google.com/search?q=testing&ie=utf-8&oe=utf-8&client=firefox-b-m

Figure 2: A screenshot of Google detecting "unusual traffic" while ProtonVPN is enabled

In any case, VPNs have the positives and negatives, but the positives largely outweigh everything else. Using a VPN is objectively safer than not. So why don't more people use them? Why don't I use mine more often?

The answer is convenience. Using a VPN on my phone results in slower speeds, as the nearest free access point is in the Netherlands (see Figures E-1 and E-2), and annoying gatekeeping, showing here in Figure 2. This is a screenshot of Google's IP verification page, which appears whenever the device's is suspected of being a webpage scraper or otherwise internet-deployed program, or sometimes when the user is using a VPN. [5] The user then must solve a reCAPTCHA (a tool to help "protect websites from spam and abuse") [6] to continue browsing. This can occur on every new browsing session and can be cumbersome enough to the point of turning off the VPN. This then exposes me to potential tracking due to my IP address not being masked. This does not mean that I am subject to doxing (a practice whereby one's private information is publicly exposed, such as their real name, address, etc.), as public IP addresses are assigned dynamically by ISPs and are constantly changing. However, I am at risk of being tracked when using free or public Wi-Fi services. Yet I have not been attacked in any way over my not using a VPN, but it could certainly happen. Personally, I doubt I will change my behaviour about this until I am able to locate a faster VPN service, which would likely end up being subscription-based.

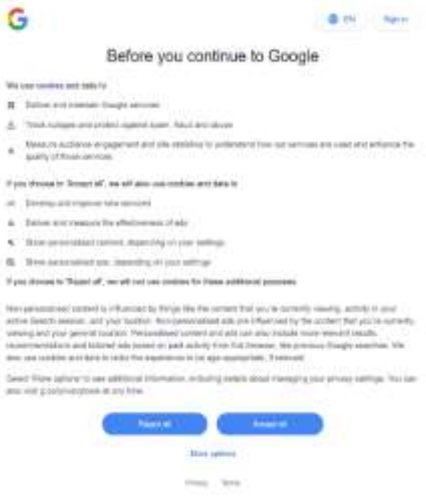
3. Cookies and “Private” browsing

I use Firefox as my browser. I mentioned above that I have a habit of using Private Browsing when searching. This is because Firefox's Private Browsing feature starts an untracked session where all cookies and trackers are deleted at the end. However, private browsing isn't fully private, as a user's Internet Service Provider can still look at the data it receives, resulting in another potential tracking point.

A web (browser, internet, HTTP) cookie is a string of information created by a webpage and stored on a user's web browser. [7] Cookies personalise a user's experience in a session by using the stored information to improve ads, remember website settings, and automatically log a user into a website. There are two types of cookies:

- Persistent cookies, which contain an expiration date and are deleted when that date is reached (or when deleted manually), and
- Session cookies, which are deleted upon the end of a session (when the web browser is closed).

Both do the same thing: they track and store the user's actions on the website to use the next time the user visits that webpage. It's obvious how this can be exploited to track users; on websites with shared logins (e.g., Google accounts to sign in on Gmail and YouTube), use several persistent cookies. A private (incognito) browser helps avoid this by manually deleting all cookies created during the session once the browser is closed. A simple way to check this is to open a website in a private window, observe its cookie statement (sometimes websites ask to put cookies, and sometimes cookies are forced upon the user), close the session, and re-open the same website. You should see that it again tells you its cookie statement (see Figure 3 and E-3). This effect is forwarded to web caching as well. [8]



Before you continue to Google

[illegible]

Figure 3: Google's cookie statement

Some downsides are that removing all cookies would result in the user signing into every website they have an account on. Websites with shared logins make this easier, but for someone like me with several across a plethora of websites, this is a nuisance. Additionally, remembering passwords becomes a new issue, and writing them down becomes a security risk. One could use a password manager (Firefox has one built-in, though there are external ones), but this then gives your password to the companies that make said managers. And again, as with VPNs: if you aren't careful enough, the company may end up stealing your data to sell to advertisers or steal your logins outright. (An example of software that combines these is The Tor Project, a free- open-source browser (Tor) built to allow people to be more private on the internet. [9] However, Tor's use for illegal sales of drugs, firearms, and other illegal items has soured its reputation among a lot of the public, generally citing the "dark web" as a reason. Additionally, its speed can be another inconvenience for people.)

However, this still isn't true privacy. Connecting to the internet requires Wi-fi (or data), which is provided by my internet service provider (ISP). ISPs are the service that allows the user to access the internet, such as Virgin Media or Eir. In order to provide this service, ISPs must process incoming data, assign you IP addresses, and log traffic. [10] Logging is the key here. Your internet history can be deleted locally from a browser or avoid storage using private browsing. But your ISP can hold onto your data indefinitely. And since it's all internet traffic, private browsing cannot stop it.

In this way, private browsing isn't all that private, since you still aren't truly hidden. However, as I stated previously, VPNs can mask IP addresses. It also turns out they can hide the user's IP address from the ISP, masking it even to them. However, the downsides of VPNs are now added to those of private browsing, making the entire situation very secure but also very inconvenient. For this reason, despite my usage of private browsing, I am still exposed to being tracked by my ISP.

Conclusion

Despite the efforts I take to stay secure on the internet, there are many pitfalls to the methods I use. Keeping one's privacy can be a very difficult thing to do as it requires changing so many of one's habits. Additionally, the requirements needed for even simple acts of privacy, such as using a VPN comes with issues I outlined above.

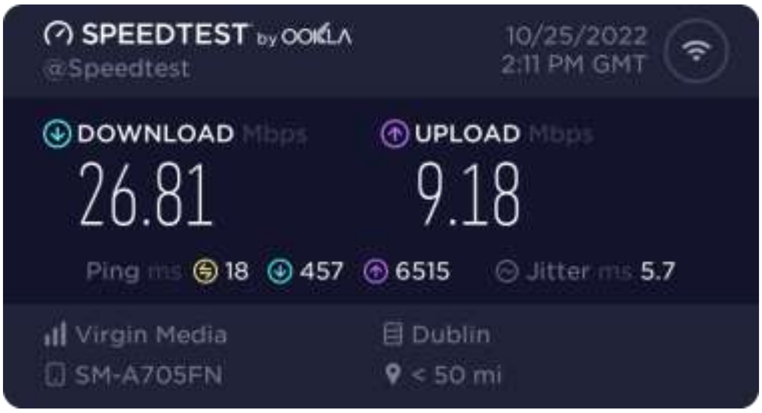
However, with the internet comes a wealth of knowledge on how to begin. There are multitudes of documents, videos, and demonstrations on setting up your server, picking a good VPN or browser, or stripping EXIF data from pictures. The changes don't necessarily need to be large either. They could be as simple as turning off your location occasionally.

In my case, while I would like to make a more proactive effort to preserve my digital privacy, I doubt I could spur myself to do so. There's always the feeling that you’ve done enough and don't need to change further. It's a special kind of laziness that many people fall into. But the fact is that I recognise the way I could be tracked online, and if I remain aware, I can take steps to stop it. I can take as much time as I need.

References

1. "What is the secure Wifi feature & how do I enable or use it", Samsung Ireland https://www.samsung.com/ie/support/mobile-devices/what-is-the-secure-wifi-feature-and-how-do-i-enable-or-use-it/ (accessed 24/10/22)
2. "What is a VPN: What Does It Do, & How To Use It (Guide) | AVG", https://www.avg.com/en/signal/what-is-a-vpn-and-why-should-you-use-one (accessed 24/10/22)
3. "Pricing | Proton VPN", https://protonvpn.com/plans?ref=tblux (accessed 24/10/22)
4. "NordVPN safe after a third-party provider breach", https://nordvpn.com/blog/official-response-datacenter-breach/ (accessed 24/10/22)
5. ""Unusual traffic from your computer network"", https://support.google.com/websearch/answer/86640?hl=en#zippy=%2Ci-shouldnt-be-getting-blocked (accessed 25/10/22)
6. "reCAPTCHA Help", https://support.google.com/recaptcha#6080933 (accessed 25/10/22)
7. "What are cookies? What are the differences between them (session vs. persistent)?", https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html (accessed 31/10/22)
8. "Private Browsing - Use Firefox without saving history", https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history (accessed 31/10/22)
9. "Tor Project | History", https://www.torproject.org/about/history/ (accessed 1/11/22)
10. "What is an Internet Service Provider (ISP)?", https://www.techtarget.com/whatis/definition/ISP-Internet-service-provider (accessed 31/10/22)

Extra Images



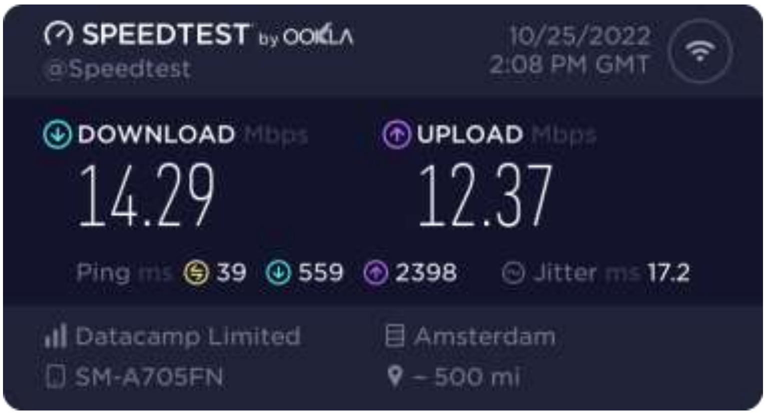
SPEEDTEST by OOKLA
@Speedtest
10/25/2022
2:11 PM GMT

DOWNLOAD Mbps 26.81
UPLOAD Mbps 9.18

Ping ms 18 457 6515 Jitter ms 5.7

Virgin Media
SM-A705FN
Dublin
< 50 mi

Figure E-1: A Speedtest.com result of my phone's Wi-fi connection while connected to my home network.



SPEEDTEST by OOKLA
@Speedtest

10/25/2022
2:08 PM GMT

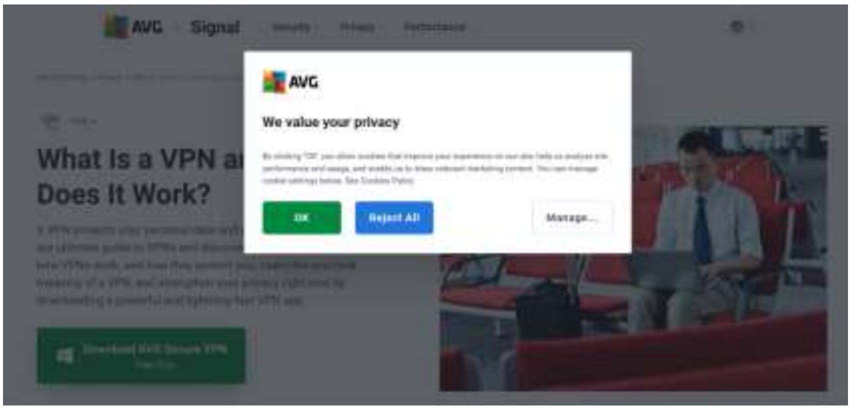
DOWNLOAD Mbps
14.29

UPLOAD Mbps
12.37

Ping ms 39 559 2398 Jitter ms 17.2

Datacamp Limited
Amsterdam
SM-A705FN
~ 500 mi

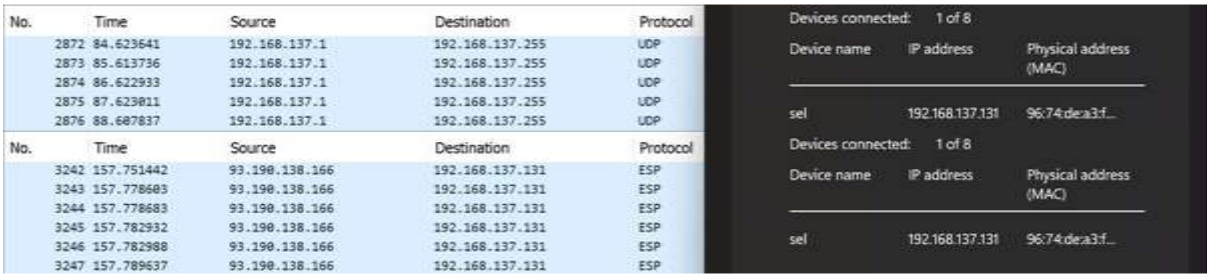
Figure E-2: A Speedtest.com result of my phone's Wi-fi connection while connected to a VPN on top of my home network.



AVG

We value your privacy

Figure E-3: A cookie statement for the website avg.com. Note its "Reject All" button the same size as its "OK" button, and the option to manage which cookies are saved.



```
No.     Time          Source            Destination        Protocol
   2872 84.623641     192.168.137.1     192.168.137.255    UDP
   2873 85.613736     192.168.137.1     192.168.137.255    UDP
   2874 86.622933     192.168.137.1     192.168.137.255    UDP
   2875 87.623011     192.168.137.1     192.168.137.255    UDP
   2876 88.607837     192.168.137.1     192.168.137.255    UDP
No.     Time          Source            Destination        Protocol
   3242 157.751442    93.190.138.166    192.168.137.131    ESP
   3243 157.778603    93.190.138.166    192.168.137.131    ESP
   3244 157.778683    93.190.138.166    192.168.137.131    ESP
   3245 157.782932    93.190.138.166    192.168.137.131    ESP
   3246 157.782988    93.190.138.166    192.168.137.131    ESP
   3247 157.789637    93.190.138.166    192.168.137.131    ESP
```

```
Devices connected:   1 of 8
Device name   IP address        Physical address
                                (MAC)
sel           192.168.137.131   96:74:de:a3:f...
Devices connected:   1 of 8
Device name   IP address        Physical address
                                (MAC)
sel           192.168.137.131   96:74:de:a3:f...
```

Figure E-4: A Wireshark capture of my phone's internet connection Before and after turning on VPN. Notice the change of protocol from UDP to ESP after the VPN has been turned on. This isn't to say that all packets are of either type; rather, the main packets sent have been changed from UDP (User Datagram Protocol) to ESP (Encapsulating Security Packet) due to the VPN. The screens to the right are screenshots of my laptop's settings showing my phone's IP address connected to by its mobile hotspot.

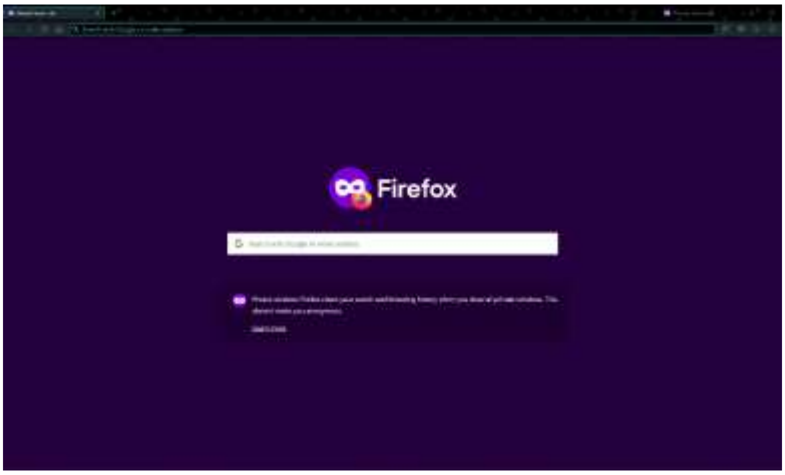


Figure E-5: A screenshot of Firefox's Private Browsing home screen.