9 ONLINE PRIVACY MYTHS KEEPING YOU FROM MAXIMUM ONLINE PRIVACY

These are the days of big data and security breaches. This is a long-distance call to action. With the risks of governments rolling back data privacy regulations and explosive data processing controversies involving social media and companies, it is clear we need to talk about online privacy.

As hot a topic as online privacy has been, most people

still fail to realize the scale and significance of the issue. Just think about it: Silicon Valley's top minds are staking up their bank accounts at insane rates mining you. Since 2010, the advertising industry tripled in size all due to the bleeding-edge data mining practices. Considering the exponential advancements of Artifical Intelligence (AI) and Machine Learning, no one is really sure what the future holds.

Taking action to secure your data is all good; however, some misconceptions about online privacy could prove to be detrimental. Hopefully, clarifying some of the most common myths concerning online privacy will allow you to maintain your data security at all times.

Private browsing mode ensure online privacy

That's a biggie, to put it lightly. Every browser has a private-browsing setting whether it's called Incognito mode, Private Browsing, or InPrivate Browsing. Though the names are catchy, the reality of the matter is not what you might anticipate.[1]

In reality, private browsing sessions do very little to protect the data you share online. Yes, when using a private mode, browsing history, passwords, searches, cookies, and temporary files will not be saved or logged. While that is great, it does not ensure online privacy in any significant way.

You might get the impression that private browsing mode conceals your IP address and virtual location. Unfortunately, that's not true in any case. In fact, each site you visit, while using private mode, can identify your IP address even if it does not have cookies to provide all the specific information. In fact, your ISP (Internet Service Provider) and other third-parties can track pretty much all your online activities with ease.

At the end of the day, private browsing modes are an automatic way to delete your browsing history but not a legitimate measure to ensure online privacy.

Public WiFi ensures online anonymity

The importance of public WiFi can not be overstated.
Having the ability to connect on the go is becoming an essential part of our daily lives, and with the increasing coverage of public WiFi, our lives are more interconnected than ever before. Unfortunately, people rarely think twice about such networks' security. What is even more concerning is the misconception that quite a few users hold - public networks to ensure online anonymity. The level of ignorance is alarming, as such claims couldn't be further from the truth.

Yes, it is true that your individual activities on the
Internet are attributed to the public network when you are connected to one. However, that has nothing to do with actual online privacy as every unencrypted connection your device makes can be tracked and recorded by snoopers or bad actors.

Now think for a
minute just how much information you share online. Yes, all that data is up for grabs, and that's a scary prospect. Highly-skilled snoopers can get their hands on your name, address, social security number, and other sensitive information by simply intercepting an unsecured public network.

Virtual Private Networks guarantee online privacy

Virtual private network, commonly known as VPN, is
quickly becoming an essential part of everyone's online experience. That's mostly due to VPN's ability to establish a secure and private connection to the Internet. By rerouting all traffic that travels between your device and the web's servers, a VPN creates a secure tunnel that is virtually impenetrable.

However, not all
VPNs can be trusted. You might have heard of a recent incident when it was revealed that in spite of a highly promoted no logs policy, the service provider allowed a third party to track down one of their user's online activities. The issue in regard to logs is a prevalent one in the VPN industry; however, most casual users do not think twice about it before choosing a VPN service.

After all, using a VPN service that keeps a record of
all your online activities defeats the purpose of using it in the first place.
You should stay away from free VPNs, as such services are often related to data collection. If logs of user activity are kept, it is highly likely that the
data might be transferred to third parties. In fact, there are not many VPNs on the market offering no logs policy, but you can find some - choose your VPN

wisely.

Internet of Things devices are not a security and privacy liability

According to the Gartner forecast,[2] the number of connected devices may reach 20 billion by 2020. The Internet of Things (IoT) market value is estimated to reach $1.4 trillion by 2021, so apparently, the industry's growth pace is not going to slow down. Every day at least 150 million data points are generated meaning hackers are given a quite impressive number of entry points to reach sensitive information.

Devices can be protected better, and that's a fact, but unfortunately, everything has its cost. Apparently, a more prominent part of potential IoT users value low pricing more than better safety solutions. We all know what the main business principle is: give people what they ask for. This is what they are doing: companies offer low prices instead of ensuring the security of users' devices, which also saves them money. However, let's not be so pessimistic - probably it's just a matter of time as IoT is still in its infancy and needs time to develop the best solutions.

You shouldn't worry about the privacy unless you hide something

Forget this. Today hackers' best interest is not exposing illegal online activities: they have their nefarious goals. Successful spying provides hackers the control of your sensitive information that may be abused in different ways you have not even thought of.

Have you ever thought that your online information taken out of the context might be used against you? For example, you can even be associated with suspicious individuals who may be total strangers to you. Thus, it is a no-brainer for hackers to do that if they have all the data they need. So, forget saying that you are not a target. If you have a bank account (most probably you do), a social security number and other sensitive data, you are a target. Actually, all of us are.

Cheap or free security tools provide the necessary protection

Usually, while choosing a product or service, cheaper

or free options are usually considered as the more attractive ones, and there is no blame in it. However, it's essential to continuously remind yourself that behind every free software or a product there is a business.

If you are not charged sufficiently or at all, most probably in this situation, you are treated as the product yourself by the service or product providers. Your data might be used for creating targeted ad campaigns and even sold to third parties. Is the product or service worth it? It's up to you to decide.

It is said that there's no such thing as a free lunch and this phrase can surely be applied here. You can find cheap or free solutions, but to ensure your online security you will need to buy some additional features for a proper piece of software. Otherwise, you may have a misleading sense of security.

Hackers target only rich people

Actually, it is the opposite. Usually, a hacker's goal is to hit as many users as possible. In such a situation, it is highly likely you could be a target. Hundreds of thousands of people may have their sensitive data leaked and, after that, a hacker only needs to go through it checking for any details that could lead to hacking into a victim's bank account with little or no trouble at all. Just imagine the consequence of that happening to you.

It is not only about the money though. Hackers may seek for copies of valuable documents, sensitive trade secrets and start blackmailing you afterwards. Your social media accounts may also be of great use.

Another argument why it is highly unlikely that wealthy people are the primary target for hackers is that they are wealthy enough to invest in hiring cybersecurity experts to protect themselves and their businesses from a severe harm that a hack could cause. It's simply easier to spy on people who have poor security practices and know little about the subject.

Private Facebook profile ensures that no one accesses your data despite your friends

Even though Facebook “Settings” gives us loads of different privacy and security options, there is a bunch of information that is always shown publicly such as name, profile picture, cover photo, username, user id and gender. You should also keep in mind that the apps you add may acquire access to your friends’ list. Even though Facebook allows you to adjust this setting, the transparency of it is highly doubted.

A scandal revealing the data of millions of users was allegedly used for political aims, put a red light on it and showed how manipulatively third parties might use our information. That is why it is critical to take your security and online privacy seriously. Carefully go through all the settings checking the information you provide about your activities as Facebook default settings[3] are highly open.

Online anonymity is impossible to achieve

Being precise, absolute 100% anonymity most probably is hardly achievable, but there are ways to come pretty near to this percentage. Using a trusted VPN service that ensures no logs policy along with professional security software, can go a long way. It is also recommended to try changing your everyday browsing habits. This way the scope of data you share with others is going to decrease.

Additionally, it is important to note that there are loads of corporations, governments (they should ensure digital rights and appropriate safeguards), and cybercriminals working hard to get as much sensitive data from people as they can for different aims, and it’s mainly up to us to decide what level of protection we want to use to ensure our online privacy and security.

The Author

Harold Kilpatrick is a cyber security consultant and a freelance blogger. He’s currently working on a cyber security campaign to raise awareness around the threats that businesses can face online.

---

[1] https://nordvpn.com/blog/incognito-mode-not-as-private-as-you-think/

[2] https://www.gartner.com/newsroom/id/3869181

[3] https://thehackernews.com/2018/06/facebook-privacy-setting.html