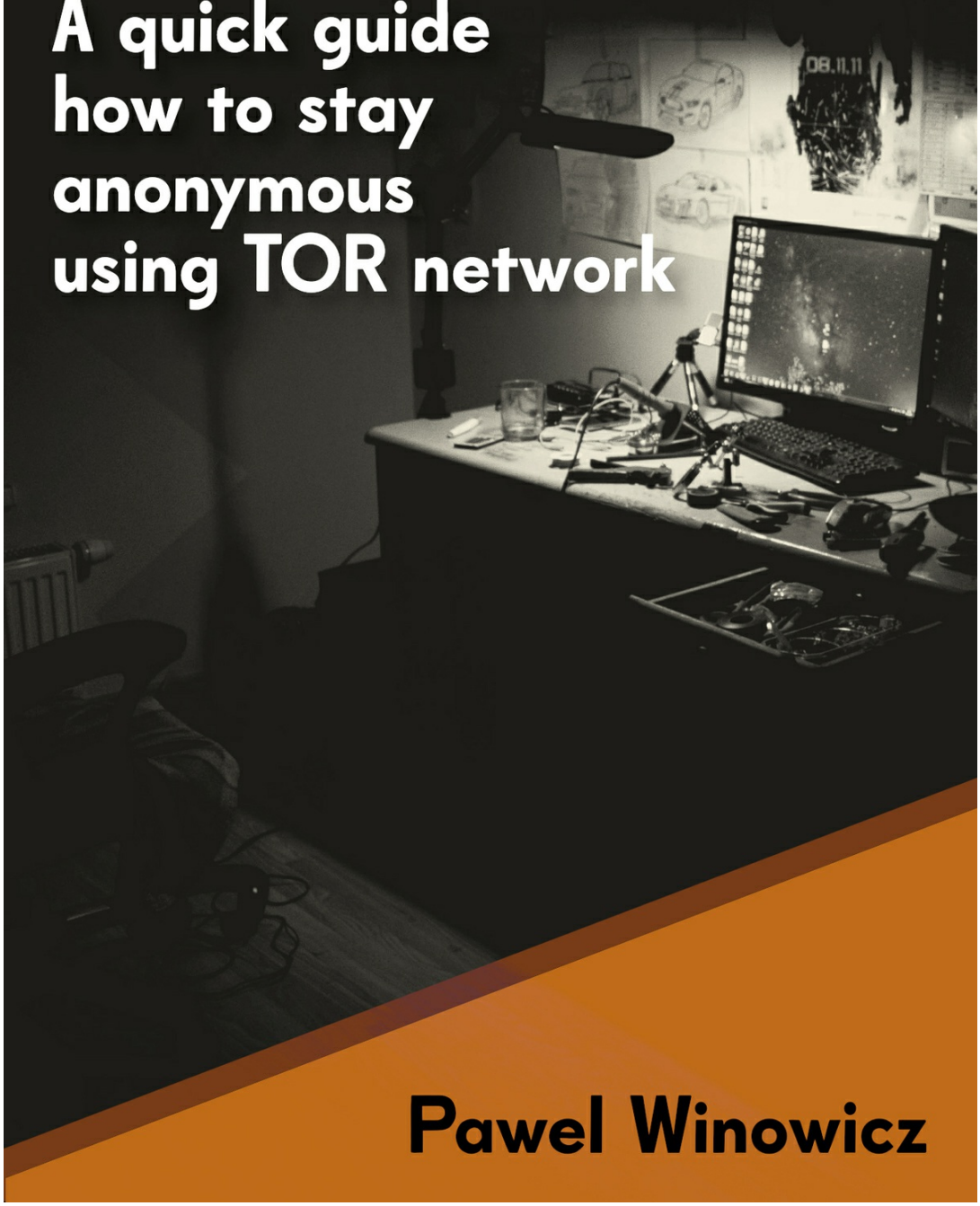
DARK WEB IN TEN MINUTES

A quick guide how to stay anonymous using TOR network

Pawel Winowicz

DARK WEB IN TEN MINUTES

A quick guide how to stay anonymous using TOR network



Pawel Winowicz

DARK WEB IN 10 MINUTES

A QUICK GUIDE HOW TO SAY ANONYMOUS USING TOR NETWORK

by Paweł Winowicz

Author book

Dark Web in 10 minutes

A quick guide how to stay anonymous using TOR network

Self-published

theselfpublisher@zohomail.eu

This guide is not intended to encourage illegal activities on the Internet, but to make users aware of how they can protect their privacy. I do not take responsibility for any immoral or illegal actions taken by my readers.

INTRODUCTION

To begin with, I would like to raise some basic issues related to the Dark Web, which will often appear in this book. Before you start with practice, it is worth to learn a bit of theory in order to better understand the principles that govern this mystical layer of the Internet.

DEEP WEB AND DARK WEB, WHAT ARE THEY?

Before we move on to discussing what a TOR browser is, how to use it and how to get to the deeper layers of the Internet with it, we need to understand exactly what Deep Web and Dark Web is. These two concepts are often confused.

So what is Deep Web?

In a nutshell, this is a layer of the Internet that we can't access from a normal browser, or we need the appropriate permissions to do so.

The things that this corner of the Internet hides include government databases, medical reports, information about users of various websites, clouds content, private videos on YouTube etc.

Most statistics show that the average Internet user is able to access only 4% of the information contained on the Internet. The entire network is often compared to a large glacier, where only part of it protrudes above the ocean surface. In this case, the ocean is the Deep Web.

What is Dark Web? Dark Web, is a small part of the Deep Web, size comparable to a web surface. The Dark Web pages are designed so that users can access them. However, special tools such as the TOR browser are needed for this. Most of the information we can find about this layer are reports of its criminal nature.

But it is not true that the Dark Web is only used by criminals. Many of the users we meet here simply value their privacy and for some reason want to hide their identity from the world.

Let us also not forget that the governments of some countries are oppressive towards their citizens and limit their freedom of expression on the Internet. In this case, using the Dark Web may be the only way to bypass censorship.

In the Dark Web we can find forums associating many human rights activists and defenders from countries where such rights are violated.

Crime and Dark Web

The TOR browser, required for surfing this part of the Internet, guarantees us anonymity and solid protection of our privacy. This creates ideal conditions for the development of crime. We can find many sites offering illegal goods - from drugs, weapons or stolen credit cards to forged passports, identity cards and licenses. While some fencees do fulfil the contract and send us the ordered, most of the websites are run by fraudsters. The preferred form of payment in the Dark Web is BitCoin, which gives the criminal even more certainty that we will not find out who he is and where he comes from.

BitCoin transactions are fully anonymous and the connection between client and vendor is effectively encrypted. Add to that the fact that we are trying to buy some illegal goods, and it makes it even easier to fool us.

We won't go to the police and we won't say - Mr. Policeman, I wanted to buy myself a pack of cannabis and a fake passport but I was defrauded. Even if we try to buy something perfectly legal there, we can't be sure that the seller will be honest. The best advice I can give you is to let go of any transactions

while on the Dark Web.

TOR BROWSER

TOR (The Onion Router) is a free open source browser designed for anonymous, uncensored communication. The name TOR derives from the onion routing developed by two US Naval Research Laboratory employees. The goal was to protect the communications of American government agencies. Further development of onion routing was taken over by DARPA (Defense Advanced Research Project Agency) in 1997, implementing it for use by the US Army.

The first versions of the browser based on onion routing were released in 2002. In 2004, the TOR code was given under a free license to Roger Dingledine and Nick Mathewson, who continued to develop the TOR project.

Does TOR offer full anonymity?

Yes, as long as we make every effort not to reveal our identity and what device we are using. Any disclosure of TOR users results from their inattention or

ignorance. All you have to do is open the file downloaded from the Dark Web through a different browser than TOR and our real location is no longer anonymous.

Safety settings

The TOR browser offers three levels of user protection: standard, safer and safest.

1. Standard - all functions of the browser and websites are enabled, this guarantees full functionality of the websites. Use the standard settings only

when browsing known, trusted sites.

2. Safer - disables potentially dangerous functions of websites. Some fonts or symbols may not work properly and multimedia such as audio and video clips only start with a click. Furthermore, java scripts are disabled on all non-HTPS pages.

3. The safest - allows websites to use only their basic functions. Scripts on all pages, even those with HTTPS protocol do not start. Many pages will be non-functional in this mode.

ONION ROUTING

This name is derived from the way data is transmitted through the TOR network. In the onion network, messages are sent with encryption layers, similar to the onion layers. The package of information sent by the user does not reach the recipient directly. This package must travel through several randomly selected computers on the network. The data is initially encrypted and then sent through a series of network nodes called onion routers. The sender of information during such a call remains anonymous because each intermediary only knows the location of the preceding and following nodes. More detailed information is available on the official TOR project website

https://www. torproject. org/

TAILS - THE OPERATING SYSTEM CREATED FOR PRIVACY

Tails is a free, real-time open source operating system focused on protecting the privacy of its users. What is a live system? It is an operating system that works directly from a flash drive or CD/DVD and is loaded into the computer's RAM.

Such a system does not use a hard drive, and therefore has no connection to data stored on our computer. When you turn off such a system, all temporary files, saved passwords, cookies and anything else that could leave a trace on us are deleted.

In the case of Tails, the remaining empty space on the pednrive is used as disk space. This allows us to save files, for example presentations or images created in the included software. Tails allows us to choose which files or program settings are important to us and saves them in an encrypted space, so we don't have to worry about losing them. All other data is deleted when the system is switched off, so that no traces are left behind.

What exactly is Tails?

Tails is a very simple and fully functional, secure operating system. It has a built-in TOR browser, Thunderbird email that encrypts the messages we send, LibreOffice, graphics programs such as GIMP and InkScape, and the OnionShare application with which we can share files and folders on the TOR network. In addition, you will find here all the tools such as a calendar,

calculator, notepad and many others.

The built-in browser offers us several plugins that can be turned on at any time and freely configured.

NoScript is an extension that, when activated, blocks any scripts that are launched when the page is opened. These can be animations, sounds, advertisements that direct to external sites, links infected with malware or tracking files. However, many sites will not work properly with the scripts disabled, so if we trust a site, we can gradually increase its privileges until we can use it easily.

uBlock is a free open code extension that blocks all ads (including infected ones) and gives us the ability to filter and block content of our choice.

HTTPS Everywhere is a plug-in that forces web pages to operate in a more secure, encrypted HTTPS

connection. If a website does not support such a protocol, it may be blocked.

HOW TO DOWNLOAD AND USE TAILS?

1. Prepare a flash drive with a capacity of at least 8GB.

2. Go to the official Tails website and download the USB image.

3. Download one of the free programs for creating bootable flash drives such as Rufus.

4. Connect the flash drive to your computer.

5. Run the program to create bootable media, enter the path to the USB image and then select the media on which you want to install the system. Confirm the settings and wait for the program to finish.

(Note - this action will delete all data from the flash drive).

6. When the program is finished, restart your computer and wait for the manufacturer's computer or motherboard screen. When this appears, click the button responsible for launching the boot menu several times. It will probably be one of the keys from F1 fo F12, this information can be found at the bottom of the previously mentioned loading screen.

7. From the boot menu, select the USB storage medium and wait for the system to load.

8. After some time you will see a window where you can change the language, time zone and keyboard type. Personally, I always leave the default settings - the less personalization, the less information about you.

In the "more options" tab we can find such settings as MAC address spoofing and connecting to a proxy server (Enabling the proxy server is useful when you come from a country where the internet is filtered and censored.)

What is a MAC address spoofing?

Apart from the logical address, i. e. IP, network cards also have their

unchangeable physical address - MAC. The above mentioned option will change the MAC address of our network card to a fake one. This will give you even more anonymity.

You will find all the details about Tails on their official website.

https://tails. boum. org/

WHY SHOULD YOU USE A BOOTABLE FLASH DRIVE AND NOT A VIRTUAL MACHINE?

Apart from the method I described above, there is another way to run such a system without using a flash drive. This can be done by virtual machine, which is an emulator of real hardware. The part of disk and memory is allocated to such a virtual machine and from now on it can be used like a completely different computer.

However, this method carries a lot of risk, an efficient hacker can come to what is above the virtual machine, speaking more technical language, who is its host and then access our real device and steal our data.

THE RULES TO FOLLOW IF YOU WANT TO REMAIN ANONYMOUS

1. Use the system installed on the pendrive instead of using a virtual machine. As I mentioned earlier, the use of a VM risks reaching information about your real hardware.

2. Do not give out any real data or any information that could lead to your identity. This does not only apply to such obvious issues as your name or age, but even to things like your favourite colours, food, brands of clothes or cars. When you're in the Dark Web, your goal should be clear - nothing stands out.

You use TOR? Great! But don't personalize this browser, it would be another element that would compromise your anonymity.

3. Do not use the browser in full screen mode. The programs adjust the size of their window to the resolution of the monitor and the settings of the graphic card. These are another data that may bring third parties closer to our identity.

4. When using the forums, use a nickname you've never used before, it's best to name yourself in the most abstract way possible. Great Bread-eater300,

JellyOfTruth_17 etc.

Think for a moment and create a nickname that you will not use outside the Dark Web.

5. If you place any comments on websites in the Dark Web, first write it down in a notepad and then paste the created content into the comment. This will help you avoid keyloggers or programs that record everything you enter using the keyboard. Yes, if it is the task of the site to collect such data, this way will not change anything. However, if the site is infected by malware, this will help us to avoid unpleasant situations such as leaks of our content to external websites.

6. When using the TOR network, do not log into your real accounts on any sites such as Facebook, YouTube, Instragram etc. Such action immediately reveals your identity, despite all layers of security you have.

7. Use the safest TOR browser mode, and use all the default plugins available whenever possible.

8. If you have a webcam or microphone, disconnect them while surfing the Dark Web. If you are using a laptop that has these devices built in, you can seal it with a piece of tape. It may sound silly, but it's worth protecting yourself in every way possible.

9. Do not install any additional browser extensions, the basic ones are enough.

HOW TO USE THE TOR BROWSER?

The first thing we should do after installing Tails and firing up the TOR browser is to enter the address check. torproject. org in the search bar.

This address leads to the official TOR project website, which checks whether our browser has been properly configured and is able to connect to the TOR network. The next step in our Dark Web tour should be to visit the Hidden Wiki. It is a set of websites, sorted by categories, accessible only from the TOR browser. The Hidden Wiki is a kind of hub of services available on the dark web.

As a warning - 99% of the pages you find here are in no way controlled by the content you upload, so you may come across really sick stuff.

The websites you visit using the TOR browser can load much longer due to the route the connection has to take. This does not apply to every side, but it is worthwhile to be patient.

SUMMARY

The basic rule you should follow if you want to remain anonymous online is to keep your mouth shut and use common sense.

No layers of security or encryption will work if you don’t follow the rules mentioned earlier in my tutorial.

Finally, I would like to thank you for reading my short book. I hope this will be a good start for you in protecting your privacy.

If you want, you can leave a review, it will definitely help me in further development.

If you have any questions or suggestions, I am here to help.

My e-mail address: **theselfpublisher@zohomail.eu**