Tor

T-O-R... Tor, these three letters raise millions of questions about this mysterious piece of software. *What is Tor? What is the Tor Browser? Is this the deep web? The dark web? *** get questions out of your face *** So many questions, and so many misconceptions!* Today, I'm going to tell you everything you need to know about Tor, why it isn't scary, and why it's such an important tool in our digital age.

Promotional Spot

The Onion Router, or Tor, is a group of servers that improve your privacy and security on the internet. *Normally, without Tor, you directly connect to a site like techlore.tech. Tor will obscure this connection by adding nodes, and every 10 seconds the chain of nodes changes without disruption to you. So unless your entry point and exit point become associated somehow, your connection is considered anonymous because of the difficulty required to backtrack in such a short span of time.*

This is all very cool. But to start, I want to clear up the biggest misconception with Tor: It's only used by criminals. Tor has an insane amount of use-cases: *It allows you to circumvent censorship, allows journalists to post in repressive regimes, gives law enforcement the power to go undercover, gives the ability to leave truly anonymous tip lines, gives support for activists and whistleblowers, and obviously, it can be used like many of you taking this course--to improve your privacy and security.* Since Tor is such a powerful tool, it is used for criminal activities. But, it's important to understand that there is an enormous amount of good that Tor does, and we can't let the bad side ruin its reputation. We will cover this misconception a bit more very soon.

The other two major misconceptions are the deep web and the dark web. What are the differences? Are they dangerous?

Well, you visit the deep web everyday. The deep web is any website that isn't indexed by search engines, *meaning you can't search for the website on a site like Google. When you login to your Reddit account, or your private email account, that webpage isn't publicly accessible and indexed by search engines, since it requires your personal information to login*. The deep web also includes private databases unavailable to the public. So I hope that already clears up the deep web, and why throwing statistics like 90% of the internet is the deep web is misleading, since it has nothing to do with Tor.

The other term thrown around is the *"dark" web*, this super spooky place...not really. Something I haven't mentioned about Tor is there are websites that require a visitor to be using Tor in order to access the site. *These are called onion sites. Instead of .com, it's now .onion. The "dark web" is any site that is an onion website.* Now, that 6% figure used to describe the *"dark web"* is also pretty misleading, since sites like *ProPublica, Facebook, DuckDuckGo, the Sci-Hub database, and Keybase, just to name a tiny few,* are all legit and legal websites that are part of the *"dark web"*. Onion sites are created for people in repressive regions to have the freedom to access these sites, one of the main reasons Tor exists.

I've been quoting the *"dark web"*, and for good reason. I dislike the name, and you should too. The *"dark web"* is a name popularized by governments and the media to make people associate it with this dark, mysterious place that's created for criminals. *Experian ads use the dark web to sell the idea that the "dark web" is used for identity fraud. This is all done to scare you into using their service--LifeLock does this as well. There was even a movie made about it.* The other crime associated with the *"dark web"* is child pornography. It does happen and it is a problem, but here's the thing...the *Internet Watch Foundation found 31,266 URLs that contained child pornography. Of those URLs, only 51 of them, or 0.2 percent were hosted on the "dark web", and 99.8% of them were found on the normal web, which you access everyday.* In reality, the actual amount of illegal traffic being pushed through Tor is most likely a much smaller number. This is why, if you ever followed me on Reddit, *I called for a rename of the "dark web", because all the name does is pollute the public perception of Tor.* I like the name private web. But any name that better represents the project and its goals for user privacy is an improvement in my book.

Now we understand what Tor is, the misconceptions behind it, and why it isn't really a scary mysterious place.....what now?

Well, there's something called the *Tor Browser Bundle. It's built on Firefox and sends your internet traffic through the Tor.* The Tor Browser functions as an anonymization tool by blending users together to look the same. This ties in with browser uniqueness, which I discussed back in lesson 3.10. As long as you're using the Tor Browser properly, which means not using your personal information in an anonymous session, and not configuring or using the browser in a unique way--you are hypothetically anonymous.

You can also access the Tor network on an operating system level to route all of your traffic through Tor, not just web traffic. You can do this by using an OS like *Tails or Whonix, two phenomenal projects that attempt to anonymize your entire system.* These were both discussed in the previous lesson.

So WOW, Tor is perfect! Well, not so quick.

First, it's not foolproof--you need to use it properly. *If you login to a personal account within an anonymous session, your anonymous session is compromised. If you install third party extensions that make you stand out from other users, you've failed. If you type or use the browser in a unique fashion, you've failed*--go back to browsing habits to learn more about behavioural analysis. The takeaway is this isn't fool proof.

Second, Tor doesn't protect you from correlation attacks, *if your attacker can watch the traffic coming out of your computer, as well as the traffic arriving at your destination, they can use statistical analysis to figure out who's doing what.*

Third, you can't control exit nodes, which may be under the control of governments or law enforcement, although there is little evidence this is a widespread problem.

Fourth, Tor is SLOW. Like...really slow. Especially if you configure it for max safety in the settings. So don't expect a speedy browser here.

Fifth, some websites won't work when you're connected to Tor. Either you'll be blocked entirely, *or sites like Google will require annoying captchas.*

The sixth and final major downside is once you use Tor, you're going to be placed on a watch-list by the FBI out of unreasonable suspicion. *ZOZ, a robotics engineer with a passion for hacking, spoke at Defcon, a hacking conference (you should definitely give this a watch by the way) and he says the more people we put on this list, the better Tor becomes as a tool to anonymize its users.* So don't be afraid of this list, you're not doing anything wrong.

Those are the major downsides. But here are some extra tips to help you out with those downsides and/or other things to watch out for.

First, be careful with third-party solutions, *and anyone who claims to give you access to Tor.* Use trusted services. Remember, the purpose of Tor is to blend users together....so simply connecting to Tor without a common fingerprint is close to useless for anonymization.

Second, the Tor Browser Bundle isn't perfect. The Tor Browser Bundle for Windows was instrumental in taking down Freedom Hosting and the Silk Road because of unpatched vulnerabilities. The safest way to use Tor is using *something like Whonix or Tails, not the Tor Browser Bundle, although it's still an excellent tool that serves its function for simple use.*

Third, avoid using the same exit nodes every time you use Tor. There is speculation that government agencies control some exit nodes, so using different ones consistently is not a bad move to spread out your traffic. *You can find a list online with possible government nodes.*

The fourth and last area of discussion is VPNs, should you use a VPN with Tor? This is widely debated, there are many different configurations out there. Here are the main ones and the pros and cons to each: *You can connect to a VPN and then route your Tor session through the VPN. This will stop your ISP from seeing the Tor session, but it will leave your exit node unencrypted and vulnerable. Adding a VPN connection at the end will encrypt the traffic leaving the Tor network, but now your ISP can see when you use Tor. There are configurations out there that allow you to add a VPN before and after your Tor configuration. Overall, if you don't know, it's better not to combine the tools.*

Let's bring everything back together. *To get proper anonymization, you should use Tor for traffic that isn't tied to your personal identity, or else your anonymous session is no longer anonymous. If you're going to do some quick research, do it on Tor so we have a good healthy amount of traffic pumping through it. If you need to do something that involves your personal identity, I would recommend using a hardened web browser, which we did in section 3.* It's not possible to make yourself anonymous, you have email accounts, bank accounts, social security numbers, so don't worry about anonymizing your personal life; worry about seperating your anonymous life from your personal life, by compartmentalizing.

To get started with Tor, *visit their website and download the bundle for your system.* If the website is blocked for you, shoot an email to Tor and tell them your situation. You should get a message sent back with the installation package. *There's Orbot and Orfox for Android, as well as now an actual Tor Browser for Android. There's the Onion browser for iPhones. Don't forget about Whonix and Tails if you want something to route your entire operating system through Tor. As for configuring the browser bundle, I made a video on my YouTube channel that goes into this.*

Before clocking out of the lesson, I want to address concerns about Tor. *There is a huge amount of discussion about whether or not it is compromised.* As of today, there is not enough reason for me to tell you it is. Almost all cases of criminals caught on Tor relied on the user making a mistake, not the direct exploitation of Tor. We are confident governments control some nodes, but we have no reason to believe they own a large amount of them. *ZOZ's talk actually addresses a lot of the concerns about Tor, so I'm going to remind you to give that*

a watch. If you're not a Tor believer, there are other projects out there designed to try and replace Tor, *most notably I2P and Freenet.*

Queue Outro Promos

This has been a very long talk, but I hope it cleared up a lot about Tor and the misconceptions behind it. I want to take this time to thank those of you who are watching this lesson, it's such an honor to be here and teach you about this project. I'll see you in the next lesson, where we will cover *anonymity relating to cryptocurrencies.* Thanks for watching.