



Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of
Meghalaya Rural Bank

Volume 2 Issue 16

Date: 16.11.2025

TOR Browser

The Tor network originated with research conducted by the United States Naval Research Laboratory in the mid-1990s, which developed the foundational technology behind onion routing. The project later released its code for public use, and in 2003 a publicly accessible version of the Onion Routing software—eventually known as Tor—became available. In 2006, The Tor

Project, a nonprofit research and education organization, was established to



oversee the network's development and maintenance. According to Tor, its mission is to promote human rights and freedoms by creating and deploying free, open-source

tools that enhance anonymity and privacy online. The Tor Browser embodies this mission by enabling users to browse the internet with a high level of confidentiality. It achieves this by routing traffic through multiple volunteer-run servers, or nodes, layering encryption in a way that resembles the many layers of an onion, which makes tracing user activity significantly more difficult. Despite these privacy-focused inten-

tions, Tor has become closely associated with the dark web, as the anonymity it provides is sometimes used for illicit activities. While the software itself is legal in many countries and was never designed to facilitate criminal behavior, some governments restrict or prohibit access to the network due to these concerns.

What is the Tor browser used for?

There are several questions worth asking about Tor, including "What does a Tor browser do?" and how its use differs from regular browsers. The Tor browser is primarily a way to browse the web anonymously. As

such, the main reason it is used is to avoid surveillance and ensure privacy while online. However, many people also use Tor to access services that regular browsers cannot reach, such as .onion sites which only function

on the onion network, such as DuckDuckGo, a privacy-enhanced search engine, which offers a .onion version of its search engine, which doesn't track user data, providing a more private search experience.

In addition, because Tor is closely linked with the dark web, some users use this for particular types of research, and also to carry out illegal activities.

How does a Tor browser work?

In its simplest form, a Tor browser uses onion routing to direct and encrypt all traffic, offering users a high level of anonymity. The network transmits traffic through three layers of international net-

work nodes called onion routers:

- Entry nodes, which form the first layer of encryption and enable the connection to the Tor network.
- A series of middle

nodes fully encrypt web traffic to ensure anonymity.

- Exit nodes, which further encrypt data before it reaches the final server.

Because onion rout-

ing effectively encrypts and relays data through multiple network layers, the Tor browser is highly effective at protecting user data and concealing IP addresses.

Benefits of a Tor browser

The Tor browser does have several advantages, which is why some internet users can benefit from using it. However, not all of these will be relevant to regular internet users. Here are some of the main reasons why some users choose to use a Tor onion browser:

- The browser is a free, open-source program
- IP addresses and browsing history are masked
- Enjoy heightened network security because the Tor browser operates on secure, encrypted networks
- Easy access to non-indexed pages, especially through search engines.

Disadvantages of a Tor browser

Aside from security concerns and wondering “is the Tor browser safe,” there are some other potential disadvantages of using this software. Below are a few things to keep in mind before deciding to use the Tor onion browser.

- Because of the way it routes traffic, Tor connections are very slow, especially when compared to VPNs, and downloading large files is not practical.
- Activity may not be completely anonymous, and it is possible to decrypt a user’s identity
- Some countries and companies can block the Tor browser, and its usage can even be illegal in certain countries.
- The use of this browser can be suspicious, even if it is legal
- Not all websites function on Tor.

How to stay safe while using the Tor browser

Many users wonder “How to stay safe while using the Tor browser?” and this is indeed a fair question. As with anything else online, there is an inherent risk with using a Tor browser. However, users can take steps to mitigate these and be mindful of their online activities. Here are a few tips for safely using the Tor browser:

- Ensure that the Tor browser and any associated apps or extensions are always up to date.
- Use the Tor browser in conjunction with a VPN.
- Employ a firewall to protect the computer’s network.
- Use antivirus software.
- Avoid logging into personal accounts, such as social media profiles or emails.
- Use the Tor browser randomly, so that it is hard to create identifiable patterns.
- Use the highest level of security available on the chosen Tor browser, so that it executes the least amount of browser code and helps protect devices from malware.
- Use an extension that protects your privacy and only accesses secure HTTPS websites, such as extensions that will automatically rewrite a URL to use HTTPS instead of HTTP.

DoT introduces new cybersecurity rules to combat cyber fraud

The Department of Telecommunications (DoT) has finalized new cybersecurity rules for the tech and telecom sectors, including major operators such as Airtel, BSNL, Jio, and Vi. These regulations aim to address the rapidly rising cases of cyber fraud. A central feature of the new framework is the **Mobile Number Validation (MNV) platform**, developed by the DoT to verify whether a mobile number is correctly linked to its user as per the telecom operators’ KYC records. This platform will enable banks, financial institutions, and insurance companies to authenticate a customer’s mobile number during account opening, strengthening safeguards against fraud. By allowing secure, direct verification of phone numbers between financial institutions and telecom operators, the MNV platform fills a critical security gap and plays a key role in preventing cybercrime.



**NATIONAL CYBERCRIME
REPORTING PORTAL**
IF YOU ARE A VICTIM OF FINANCIAL
CYBER FRAUD VISIT cybercrime.gov.in
OR DIAL HELPLINE NUMBER 1930

**HELPLINE
NUMBER
1930**