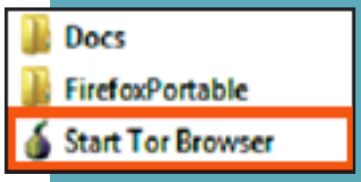
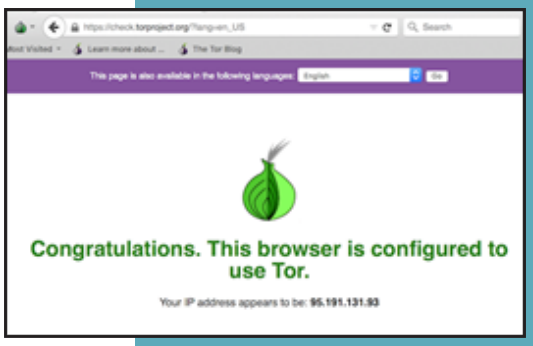
USING TOR TO ANONYMIZE YOUR ADDRESS

Tor Browser is a free, open source web browser that uses a volunteer network of virtual tunnels and a layered encryption process to anonymize your IP address. Note that Tor anonymizes the origin of your traffic and encrypts everything inside the Tor network; however, it cannot encrypt the data after it comes out of Tor at the destination. Tor can be installed according to the instructions to the right.

1. Visit torproject.org. Download and Install the Tor Browser Bundle to your hard drive or a flash drive.

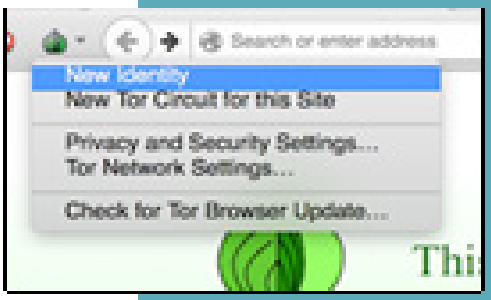


2. Launch the Tor Browser which can be found at the location you saved the bundle to. Double-click "Start Tor Browser".



3. Ensure your Tor Browser is providing you with an anonymous IP address.

4. To use a new IP address, click the drop down menu ith the onion next to it and select "New Identity". Please note that doing this will close all of your currently opened tabs.



Best Practices

- Do always use a secure browser and VPN that anonymizes your IP address when accessing anonymous email services. Be sure your browser is updated regularly.
- Do remember, although the tools anonymize you, if you have to pay with traditional means, you can be identified through that transaction.
- Do use VPN services. They anonymize your IP address, although you will have to submit personal data to sign up for the service.
- Do not access more than one account in a single browser session, and never access popular services such as Google or Yahoo in the same session.
- Do not include personal details in your communication that can be used to identify you, such as your name, phone number or address.
- Do not use anonymous email services on any device that requires personal logins, such as a smart phone with linked accounts.

Warning! Tor is generally used when someone needs to hide their computer's identity or location. It should not be used as a default search engine for everyday internet browsing. Never visit social networking sites or enter any personal data on any website using the Tor Browser — it is poorly regulated and leaves your information extremely vulnerable to theft.

ANONYMOUS INTERNET & MESSAGING SERVICES SMARTCARD

TYPES OF MESSAGING SERVICES AVAILABLE ONLINE

Provider	Service	Primary Use	Data Retained	Data Sharing	Cost
Hide My Ass!	VPN Temporary Email	Freely surf the web (VPN). Receive emails and use the inbox for websites that you do not necessarily trust that require you to provide an email address.	IP address, cookies, payment details, username, password, and actual emails. HMA asks for an existing email address at signup but this is optional.	They do not sell personal data to 3rd parties unless required by law. They do share information with members of AVG Group.	VPN as low as $6.99.
CloakMy	One time message and chat service	One time messaging and chat. You have to send the recipient a unique URL to go retrieve the message.	Logs IP addresses	None, does not share or sell information to others	Email is free.
ProtonMail	End to end encrypted email	Fully encrypted email, emails are encrypted client side so they are fully encrypted when they get to the Proton servers in Switzerland	Optional additional email upon sign up for account recovery purposes.	Proton if compelled, could only hand over encrypted emails. They do not retain the keys to encryption, the client does.	Free
HushMail	Email Host	HushMail is an email host just like Gmail or Yahoo. It is accessible through Tor and it does not require personal information to register.	Browser type, operating system, IP address, credit card information when purchasing product. Retains email messages for up to 18 months, encrypted or non-encrypted.	Logs user IP addresses. They have also turned over user data to U.S. authorities in the past due to court orders.	Free
Signal	Encrypted text messaging	Send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls	Signal users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message. Signal says it will share information with Third Party service providers, and for legitimate legal purposes.	$49.98/year
Wickr	Encrypted text messaging	End-to-end encryption and content, expiring messages, including photos, videos, and file attachments and place end-to-end encrypted video conference calls	Wickr users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message	Free
Mailinator	Temporary disposable Email	Use the Mailinator address anytime a website asks for an email address. Can only receive email.	No signup required.	Mailinator is a public domain so anyone can read an email if they know what address was used. Use odd names to avoid heavily used inboxes.	Free

There are many email and messaging options out there that can provide a means to send and receive messages anonymously or semi-anonymously. The right service for you will depend on the primary nature of your communications , the cost, and the information you are willing to provide.