

Anonymous Email Services- Do's and Don'ts

- Always use a secure browser that anonymizes your IP address for accessing anonymous messages.
- Do not access more than one account in a single browser session, and never access named accounts, such as Google or Yahoo in the same session.
- Do not include personal details in your communication that could be used to identify you, such as your name, phone numbers, or addresses.
- Use public WiFi for additional anonymity and never repeat usernames or passwords.
- Remember, no set of tools can guarantee anonymity.

Using an Anonymous Email Account

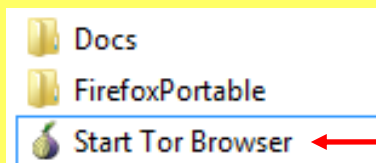
Anonymous email services can be used to send personal or work-related messages without leaving a trace of your identity. Anonymous email accounts require no personal information to register and retain little usage data. They should always be accessed and used **in conjunction with an anonymous IP address.**

Using Tor to Anonymize Your IP Address

What is Tor?

- Tor is a free, open source web browser that uses a volunteer network of servers and a layered encryption process to **anonymize your IP address**
- Before you access an email service, you must download and install Tor to protect your device's unique IP address
- Tor does not protect the information transferred between the Tor Network server and your destination site

- 1 Visit torproject.org and download the **Tor Browser Bundle** to your hard drive or a flash drive.



- 2 Open *browser.exe* in Windows Explorer, then open the new *Tor Browser* folder and double-click **Start Tor Browser**.

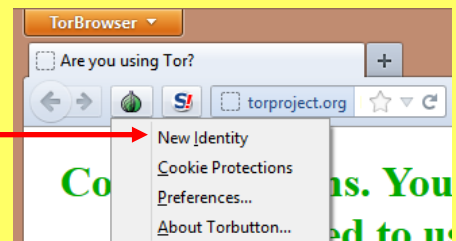


- 3 Make sure your Tor Browser is providing you with an anonymous IP address.

Tor will display your device's IP address as it appears online.



- 4 At times, you may have to change to your Tor-generated IP address. You can renew a different IP address by going to **Green Onion > New Identity** in the top left corner of the Tor Browser.



Choosing the Right Anonymous Email Service

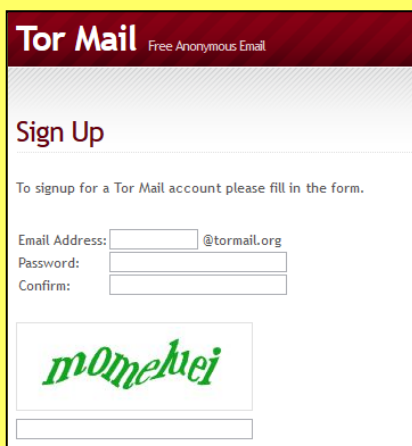
The following services can be used to send and receive messages without leaving a trace of your identity. These four services specialize in security and privacy, have simple sign up processes requiring no personal information, and divulge account data only under rare circumstances, if ever. The right service for you will depend on the organization providing the service, frequency of your use, and the primary nature of your communications.

Service	Organization	Service Type	Data Retained by Service	Data Sharing Policy	Cost	Suggested Frequency	Primary Use
Tor Mail (tormail.org)	Unknown (Note: not hosted by a known/trusted entity)	Webmail	Unknown	No 3 rd party sharing	Free	Weekly to monthly access	Scheduling in person meetings, casual correspondences
Hushmail (hushmail.com)	Hush Communications Canada, Inc., Canada	Webmail	IP address, <i>purchase information*</i>	No 3 rd party sharing unless issued a court order	Free, opt-in Premium option	Daily to weekly access	Scheduling in-person meetings, private correspondences, press communications
Lavabit (lavabit.com)	Lavabit LLC, Texas, USA	Webmail	IP address, browser type, sender/recipient email address, time stamp	No 3 rd party sharing unless issued a court order	Free, opt-in Premium Option	Weekly to monthly access	Scheduling in-person meetings, private correspondences, press communications
Cloak My (cloakmy.org)	Webmy.me Inc, California, USA	Message and chat	IP address, session cookies	No 3 rd party sharing	Free	One-time correspondence	One-time messaging and chat, no account required

* name, account and domain, alternate email, billing address, credit card information, IP address of purchase, for premium accounts.

Tor Mail – Creating an Account and Picking Webmail Client

1 Use the Signup screen to fill out Tor Mail's registration information and complete your sign up.



Tor Mail Free Anonymous Email

Sign Up

To signup for a Tor Mail account please fill in the form.

Email Address: @tormail.org

Password:

Confirm:

momehei

2 Use the Log in screen to access Tor Mail's webmail client to send and receive emails.

When you login you must login with your USERNAME and NOT your EMAIL.
Correct: username
Incorrect: username@tormail.org



Control Panel



Round Cube Webmail
Requires Javascript



Squirrel Mail Webmail
No Javascript

Always use
Round Cube
Webmail.

Lavabit – Creating an Account and Optimizing Preferences

1 Navigate using the menu found on the Lavabit homepage.



Username:

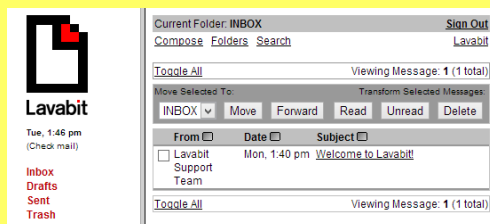
Password (Once):

Password (Twice):

Security Code (Below):

2 Fill out the required fields in the **Sign Up** menu and select the ad free account option.

3 The **Webmail** menu allows you to access the Lavabit Webmail client to send and receive messages.



Advanced Options

Require SSL: Enable ☒ Disable ☐

Accept Bounce Messages: Enable ☒ Disable ☐

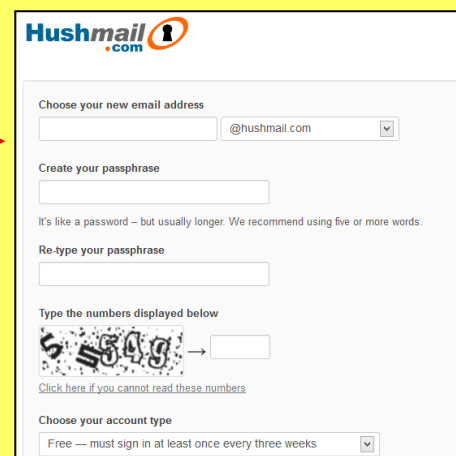
Automatically Rollout Old Messages: Enable ☒ Disable ☐

Save | Return to Main

4 Navigate **Preferences > Advanced Options** and enable the **require SSL** field.

Hushmail – Creating an Account and Using Tor

1 Fill out Hushmail's required registration information and create an account.




Hushmail.com

Choose your new email address
 @hushmail.com

Create your passphrase

It's like a password – but usually longer. We recommend using five or more words.

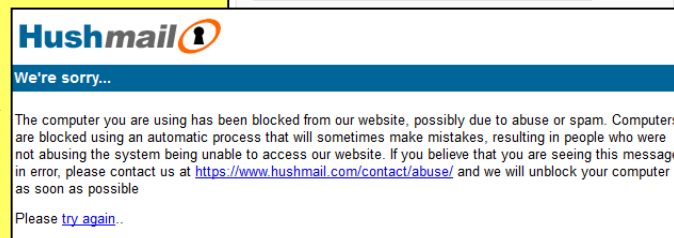
Re-type your passphrase

Type the numbers displayed below


Click here if you cannot read these numbers

Choose your account type
Free — must sign in at least once every three weeks

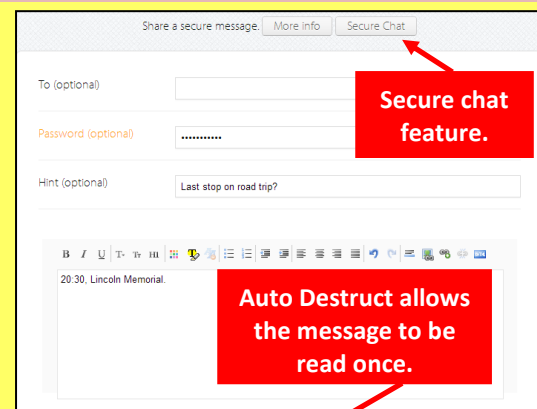
2 If you see the following message when attempting to sign in to your Hushmail account, you must use a new Tor Identity (see step 4 on the previous page).



3 You can login to Hushmail's webmail client on the top right of the Hushmail homepage to send and receive messages.

Cloak My – Sending Messages and Options

1 Enter the desired message. Supplemental information is optional.



Share a secure message. | More Info | Secure Chat

To (optional):

Password (optional):

Hint (optional):

20:30, Lincoln Memorial.

Expiration: ☐ Auto Destruct ☒ Timed ☐ Never Expire

Start Date:

Send Message

Secure chat
feature.

Auto Destruct allows
the message to be
read once.

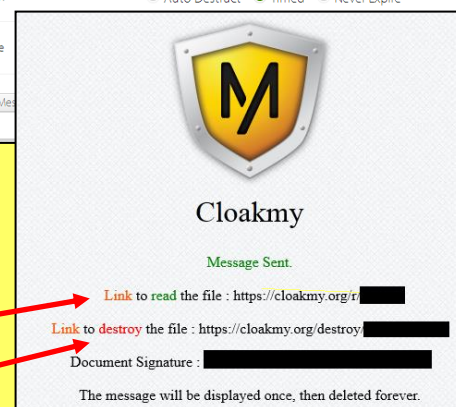
2 Choose an expiration setting for the message.

3 After the message is sent, a unique URL location is created for the message.

4 You must distribute this URL to the recipient. Only a user with this URL can view the message.

Read Message

Destroy Message



Useful Links

A Parent's Guide to Internet Safety
Privacy Rights Clearinghouse
Microsoft Safety & Security
OnGuard Online

www.fbi.gov/stats-services/publications/parent-guide
www.privacyrights.org/Online-Privacy-and-Technology
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx