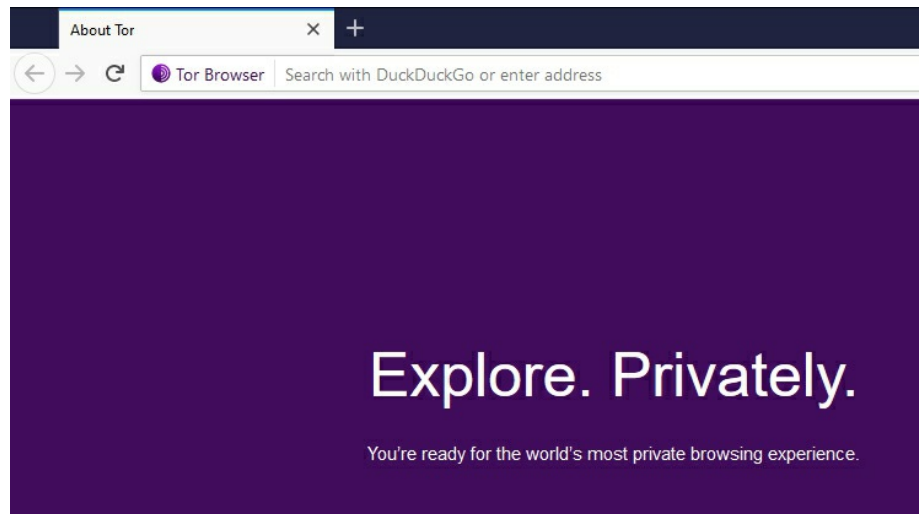
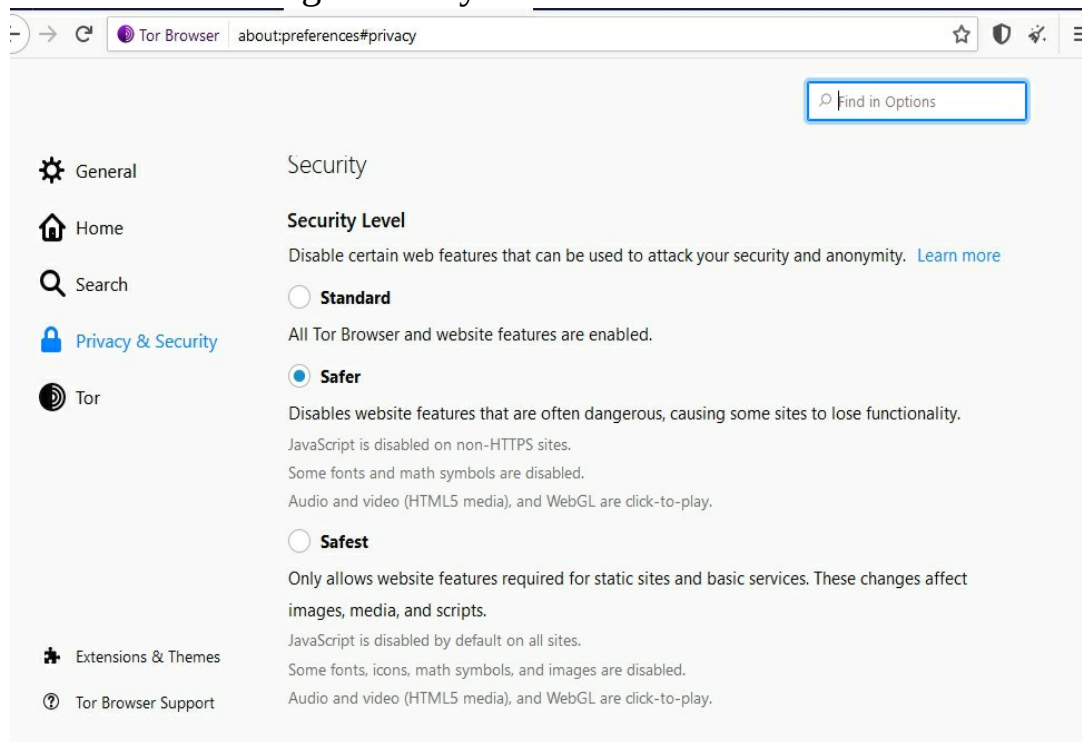


Getting Started with Tor

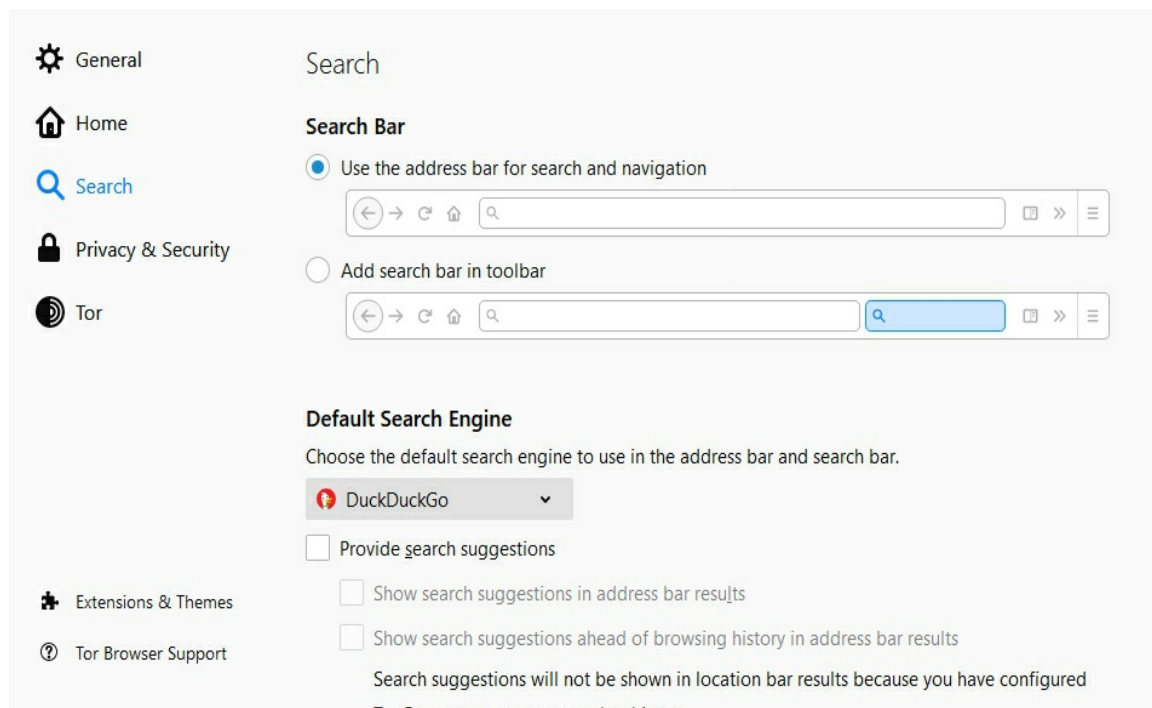
Tor is quite easy to use and the following tutorial will get you up and running with the browser. You will configure all of the important settings and use built-in tools to keep you secure and safe online.



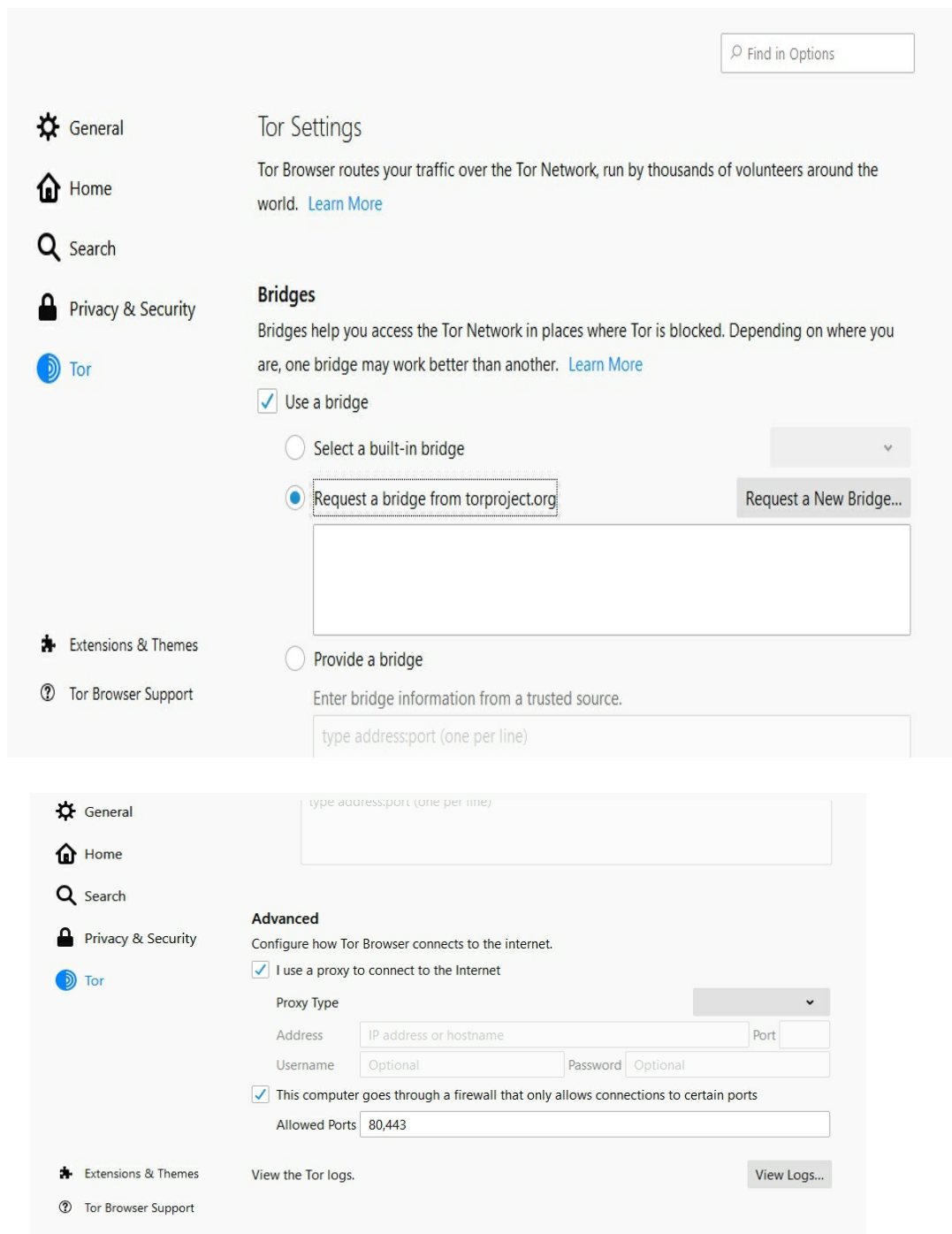
1. Install and run Tor, and opt to connect directly to the Tor network. Click the onion icon in the top left of the address bar before you start browsing. You will be able to change the 'circuit' nodes through which your connection is routed.



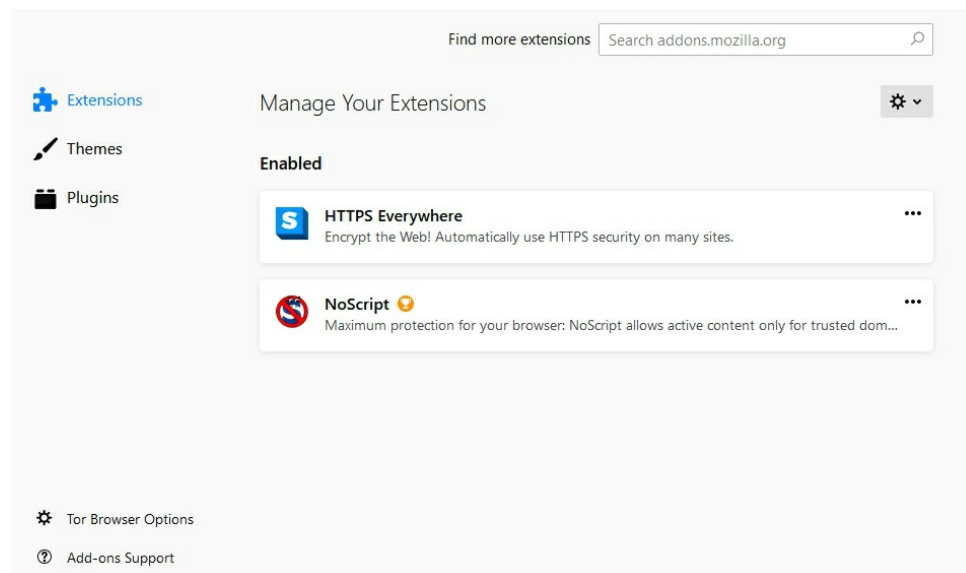
2. On the menu in the right-hand corner, click on options. Click on privacy and security settings to set your security level. Tor will be set at Standard as default, this may leave you compromised. Safest will make the web look a little bare, so Safer might be the best balance between security and features. It will also disable javascript which if left enabled provides hackers with an entry of attack.



3. To change Tor's search engine from the default DuckDuckGo, click on 'Search' from the Options menu and then click and then select a search engine from the drop-down menu below 'Default Search Engine'. There are several other alternatives depending on your preference but DuckDuckGo is commonly used with Tor.



4. Sometimes the '.onion' sites won't load when accessed via the address bar. If this happens select the onion icon and choose Tor Settings. Select the ISP option to connect using secret entry nodes 'bridges'; or computer options to connect via a proxy.



5. The 'Extensions' option in the menu in the right-hand corner of the browser will allow you to add certain features to the Tor Browser according to your preferences. The HTTPS Everywhere add-on is important and should always be used because it converts every website with HTTP to a secure HTTPS. The NoScript add-on is also important as it will block scripts on some websites that would otherwise compromise security.

Tor Extras for Safe Surfing and Purchasing

Tor will require other software in order to ensure complete anonymity when surfing the internet. Just using Tor on its own is not enough and you could still be vulnerable. The following extras I recommend are:

VPN

A virtual private network (VPN) can offer extra encryption to your surfing privacy using encrypted proxy connections like Tor. It will guard your IP address from the Tor entry node and your Internet Service provider will not know what you are doing on the net. If you want complete anonymity then using a VPN along with your Tor browser is a good start. Using a VPN is one of the best ways you can protect your privacy. You can purchase VPNs with fully-enabled features such as multiple IP addresses and locations to choose from. You can also download free versions that will have enough features that you require to stay private but you won't have as much choice on the location of the IP address and you may have to wait in a queue to connect.

ProtonVPN is an excellent free VPN tool that will secure your connection with the strongest of encryption. The free version will limit you to only three countries of choice and connection speed is slow but you can upgrade to paid plans that will give you more features and privacy. Windscribe is another excellent VPN but the free version will limit the data usage to 10GB per month. CyberGhost is another VPN that provides an excellent service but there is no free version. It is the VPN that I use. The paid versions of VPNs is always the way to go if you want extreme security on your network. Free versions will always leave you vulnerable and cannot guarantee full security from attacks and governments may still get hold of your IP address.



Anonymous Email Services

Messages won't be encrypted using a normal messaging service and anyone intercepting them will know your name and real address. Using a Tor-enabled email service such as ProtonMail will provide total anonymity and privacy. ProtonMail, launched by the CERN research facility in 2013, is an end-to-end encrypted email provider. ProtonMail introduced a hidden service for Tor combating against censorship and surveillance. There is a free version with limited storage and messaging or you can upgrade to a paid plan for advanced features. Bitmessage used to be another email service that could be used with Tor but vulnerability was detected and the software was compromised. But we will explore ProtonMail a bit more, as many cyber security specialists choose it as their email provider.

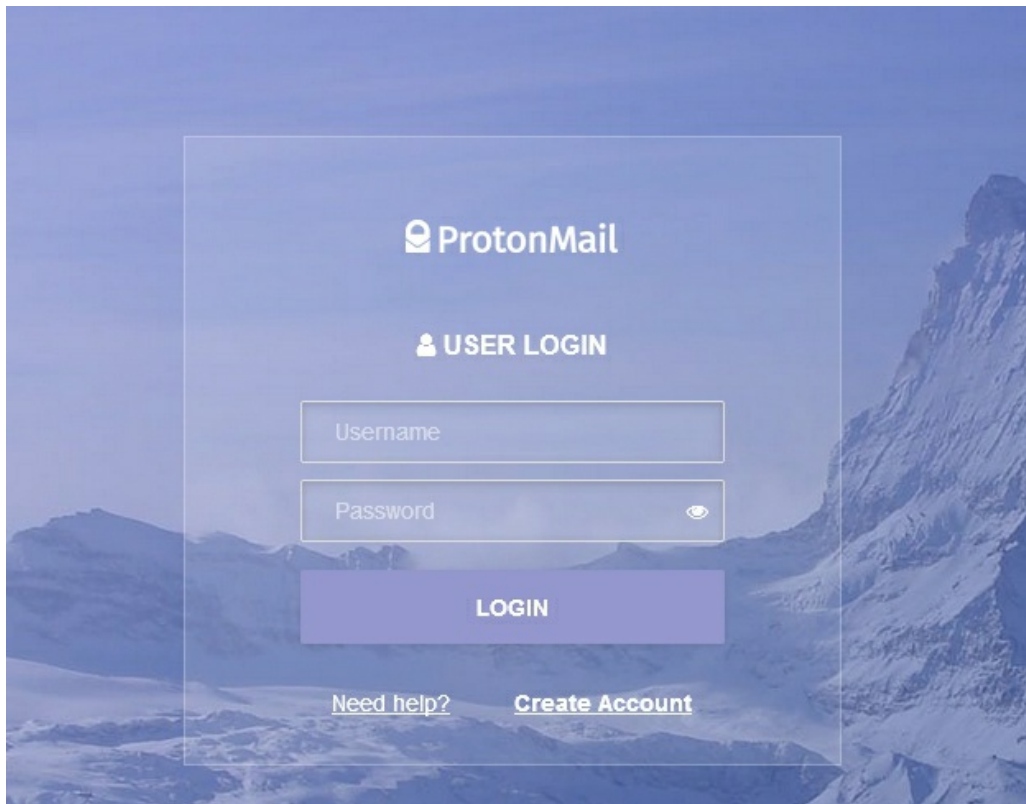


ProtonMail should be your go to for setting up secure, extreme privacy email accounts. Now the main features that should entice you to use it as your provider of choice are that it offers end-to-end message encryption. This means from the moment it is sent to the moment it is received, it is encrypted and no one can see it including the people working for ProtonMail itself. That is the fundamental reason to use ProtonMail because services like Gmail, Outlook and Yahoo, while secure to the outside world, can be viewed by people working on the service. Email addresses can be scraped and sold to third-parties for marketing purposes which is a major downer.

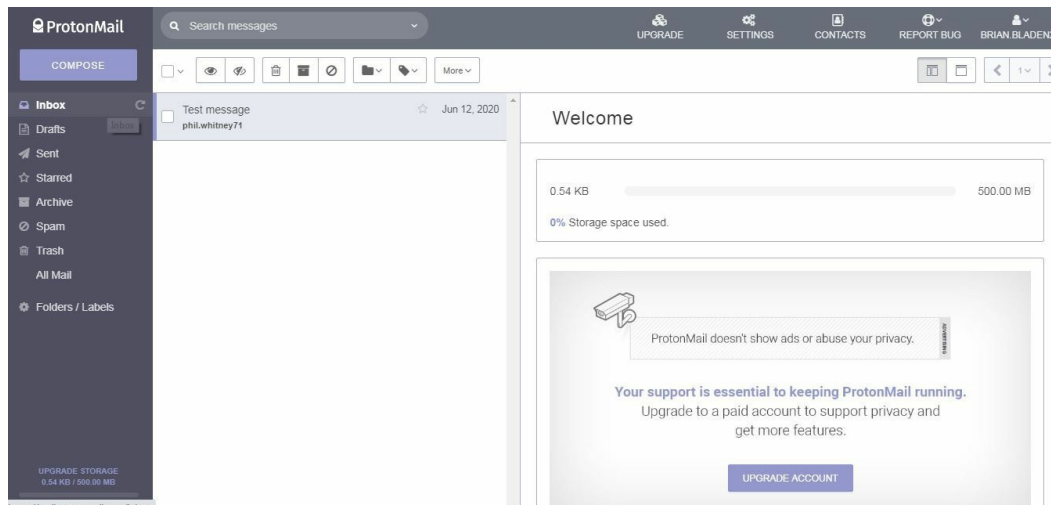
Governments can demand your email and password information, too. The service avoids pressure from governments because the technology used simply does not allow the company to disclose data. And they do receive constant requests. So ProtonMail is definitely a wise choice as your main email provider. ProtonMail is a Swiss based service and its development was financed through crowdfunding. It offers paid tiers but across every tier, including the free version, the email service has the same level of security.

This book will not be covering the advanced features that come with the paid plans but I would say the main one is that you can use a custom domain and

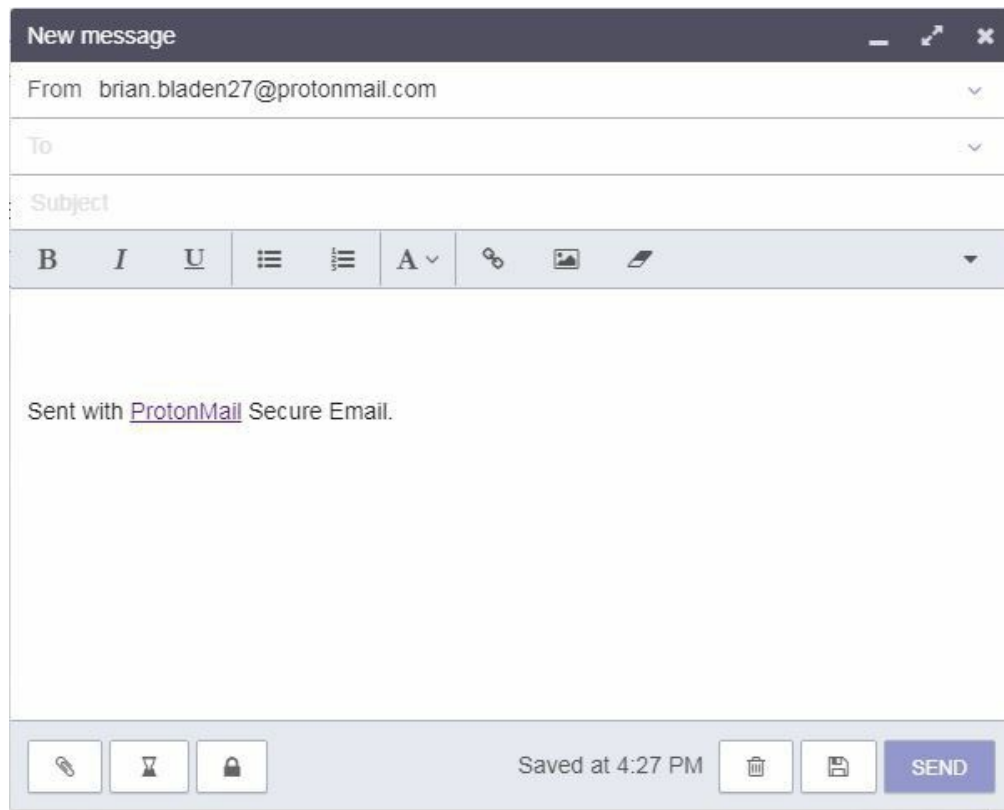
email address for the account. This is an excellent feature for creating email under aliases. This book will cover the main features that come with the free version. The software does not store any IP logs, so there is no data for someone to sift through. It is easy to use and has a clean interface. The interface is customisable, although if you use custom themes it may leave your privacy compromised.



On the sign-up and login, what makes this a great service is that it doesn't ask for any personal information. You can create the email with a different name other than your own so you could put John Doe in the email address if you wanted. The account would be created in minutes, no requirement for mobile phone numbers and addresses.

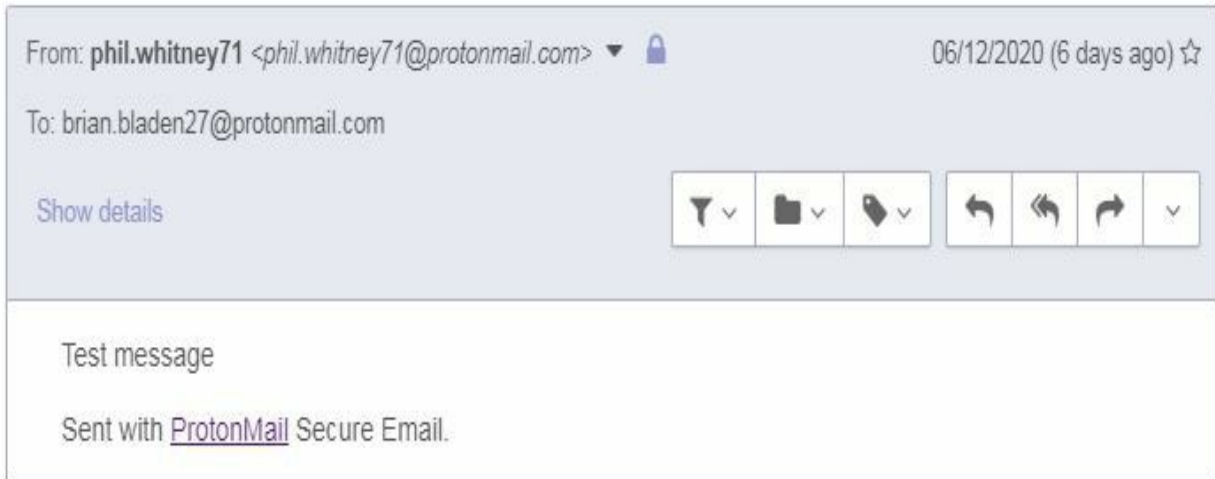


The image above shows the interface of a ProtonMail Account and its navigation. This screenshot shows a test account that I had set-up for training purposes. As you can see it is a very clean layout and similar to other email service providers. Down the left we have the usual folders like inbox, drafts, sent box, archives and trash. The list of emails sent to your inbox is the main segment in the centre of the page and when you click on the email you see the body of the message to the right, along with email addresses. To write a message you click the compose button top left. And a message box will open up for you to write your message with a subject line and body of the message.



To test the service, a message was sent to this ProtonMail account from another Protonmail account. The message received was pretty much the same as any other provider, you have the 'to' address and the 'from' address and the message below. In the screenshot below of the message, you can see there is an icon of a padlock to the right of the 'from' address.

Test message



This indicates that the message was end-to-end encrypted. If the message had come from someone who was using another email provider, say like Gmail or Outlook, then the message would not have been encrypted. As the message was sent between two ProtonMail accounts then it was end-to-end encrypted. If a message was sent from a ProtonMail account user to another person using another service provider, then it may still be end-to-end encrypted. I will explain to you how to do this.

New message

Encrypt for non-ProtonMail users ⓘ

Message Password

Confirm Password

Password Hint (Optional)

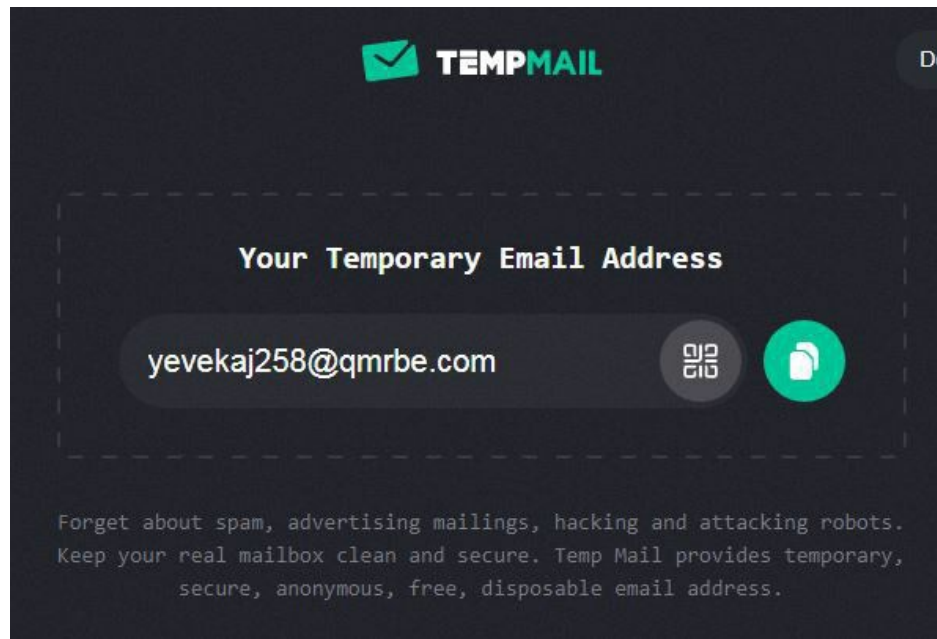
Encrypted messages to non-ProtonMail recipients will expire in 28 days unless a shorter expiration time is set.

CANCEL SET

When you click compose to write your message, the box will appear for you to type your addresses, subject and message. If you scroll to the bottom you will see that same padlock icon. When you click on it, you can set a password as shown in the image above. The person receiving the email would only be able to access the message by using this password. So you will be secure at both ends. That is really the basics of using this email service and it is a great way to keep your online communication secure, with extreme privacy. A ProtonMail account is also a great option for use with logins for all of your online accounts such as social media and online banking.

Disposable Email Address

Should you use your own email address then you are defeating the object of staying anonymous. Whilst you are browsing anonymously surveillance may be able to see the real email address you have entered. It is best practice to use a disposable email service to create a temporary email address for site registrations and keep your Tor persona separate from your real web information. A good email provider is Temp Mail that can provide you with a temporary email address. An alternative is Guerrilla Mail.




Cryptocurrency Wallet

If you intend to use the Tor browser to buy and sell things then you are going to need cryptocurrency such as Bitcoin. Using a wallet can provide you with a safe account to store your currency and have access to useful data such as the current market price. Blockchain is a popular Bitcoin wallet and it has a HTTPS certificate (most onion sites do not have this) for added security for your savings. A good alternative is Green Address which has excellent security features and instant confirmation of transactions.

DuckDuckGo

It may be the Tor's default search engine but it is worth mentioning what it does. DuckDuckGo will allow you to search the web without being spied on, taking advantage of the anonymity of Tor. It also has a useful feature where you can use abbreviated commands to search sites, such as !w for Wikipedia followed by a search topic. An alternative search engine that won't compromise your privacy is Startpage.




[Web](#) [Images](#) [Videos](#) [News](#)

All Regions ▾ Safe Search: Strict ▾ Any Time ▾


Home - BBC Sport

The home of **BBC Sport** online. Includes live **sports** coverage, breaking news, results, video, audio and analysis on Football, F1, Cricket, Rugby Union, Rugby League, Golf, Tennis and all the main world **sports**, plus major events such as the Olympic Games.

 bbc.co.uk/sport [More results](#)


Football - BBC Sport

The home of Football on **BBC Sport** online. Includes the latest news stories, results, fixtures, video and audio.

 bbc.co.uk/sport/football


BBC Sport (@BBCSport) | Twitter

The latest Tweets from **BBC Sport (@BBCSport)**. Official <https://t.co/XsBH2P4slh> account. Also from **@bbc** - **@bbcmotd** **@bbcft** **@bbctms** **@bbctennis** **@bbcrugbyunion** **@bbcsnooker** & **@bbcgetinspired**. MediaCityUK, Salford

 <https://twitter.com/bbcsport>

BBC Sport

bbc.co.uk/sport



BBC Sport is a department of the BBC North division providing national sports coverage for BBC Television, radio and online. The BBC holds the television and radio UK broadcasting rights to several sports, broadcasting the sport live or alongside flagship analysis programmes such as Match of the Day, Test Match Special, Ski Sunday, Today at Wimbledon and previously Grandstand. Results, analysis and coverage is also added to the BBC Sport Website and through the BBC Red Button Interactive television service. [More at Wikipedia](#)

Hiding Tor from your ISP

Many Tor users are worried that their internet service provider (ISP) will know that they are using Tor. It is possible for ISPs to be able to detect when you are using Tor and could potentially notify law enforcement agencies. There are several methods you can use to hide Tor from your ISP and some of them are technical so you may need some assistance.

Bridges

Tor bridges, or sometimes known as Tor bridge relays, are alternative entry points to the Tor network. This will make it harder for the ISP to know when your system has entered the network, but not impossible. The Tor Project website has bridges available for you to use and configure with your browser. I recommend visiting a few sites that I have listed at the end of this guide that can assist you in using bridges.

Pluggable Transports

ISPs have found ways to block Tor even when using bridges. Censors used with ISPs can peek at network traffic and detect Tor; thus blocking the flow of traffic. Tor has introduced pluggable transports, also known as obfuscated bridges, which can circumvent the censorship. This is quite a new technology that Tor is implementing. The technology will attempt to transform your traffic into innocent looking traffic to the ISP and censors. The definition of obfuscating is to hide the intended meaning of communication making it hard to interpret and ambiguous. The plugins will basically use a protocol to transform your traffic into random pockets of data. This technology will certainly guard against your ISP; although law enforcement may be able to get a sniff that you are using Tor at the initial engagement between computer and the obfuscated bridge. To obtain an obfuscated bridge, or pluggable transport, you will have to email Tor as they are not easy to get.

Flash Proxy

The Tor browser has the 'flash proxy' built in through Javascript and WebSockets that can help censored internet users. Tor bridge relays can be blocked even though only a few IP addresses are handed out at a time. The flash proxy will create many IP addresses that censorship will not be able to

keep pace and block them. The flash proxy will not increase bridges at static addresses; rather they create a large and ever changing pool of addresses. The tor client will contact the flash proxy facilitator to communicate that it wants a connection. The flash proxy facilitator will keep track of clients and proxies and match them up to one another. The more people use Tor and become bridges the more options the flash proxy has, which help to prevent surveillance keeping track of the connections.

VPN

VPN is the easiest method to use and can be used with Tor to boost your privacy. The downsides of using VPN is that the provider can see what you are doing and can potentially report you and the speed of your connection, whilst secure, will be slow. It is best to connect to your VPN first selecting the IP address and location you desire before connecting to the Tor browser. If you choose to connect to Tor first then you will need to configure the VPN so that the browser works with the VPN and there are not many VPN providers that can do that (AirVPN being one of the few).

Tor Tips – the do's and don'ts

This section explains what you should do and what you should not do with your Tor browser in order to stay anonymous and safe. Tor was developed through funding from the US Government and has been an effective tool for investigative journalists and whistle-blowers who wish to keep their contacts and information private. Today, Tor is used by normal civilians guarding their privacy and criminals looking to trade on the dark web. Below are explanations of how to make the most of the Tor network and how to avoid pitfalls too.

Do update your Tor browser as soon as an update notification pops up on the browser. Although Tor is more secure than Chrome or Firefox browsers it does not mean it is impervious to a hacker on the attack. Tor addresses threats and vulnerabilities, so it is essential that you keep the Tor browser up to date.

Do not maximise the Tor window because maximising allows websites to determine the size of your monitor. This on its own may not sound worrying but if it is combined with other information websites may be able to identify you.

Do use a Virtual Private Network (VPN) alongside the Tor browser. Tor only protects traffic routed through the browser it is not a VPN. You can boost your security and privacy by using the VPN in conjunction with Tor. The VPN will ensure all your data is encrypted and no logs are kept of your browsing activity.

Do not use Tor for torrenting to download and upload files. Tor may seem like a perfect privacy tool but using software such as BitTorrent and other peer-to-peer networks will affect your anonymity. Your real IP address will be sent to the torrent service and other 'peers'. They will then be able to identify you and view the data you are sharing. File-sharing is not encouraged by Tor and exit nodes are configured to prevent torrent traffic.

Do create a new identity because some websites will try to track you even while using Tor. Tor will usually warn you when a site is trying to do this and gives you the option to choose a new identity by clicking on the onion icon.

Do not share your real email address, which is an obvious way of giving your identity away on the Tor network. Use a disposable email address service such as Fake Name Generator or MailDrop. You can use these services for temporary addresses when registering on sites.

Do not search the web using Google in Tor as they do not respect your privacy. By doing this you are defeating the object and giving away your anonymity. Google will track your browsing and make it difficult to use its services due to your 'suspect' manner of connecting. Sign-ins will require CAPTCHAs that ask you to prove you are not a robot, which is very irritating.

Do think about running a Tor relay to help the browser remain anonymous. The ever expanding community of Tor users are relied upon to provide the relays that create circuits. These circuits keep the browser anonymous. However, if you intend to run a relay you will need a Linux computer running Debian. If you operate with Windows then you will need to run a virtual machine with Linux and set up the relay from it. You should consider running a 'middle relay' rather than an 'exit relay'. Middle relays do not show your IP address as the source of traffic. An exit relay will and if anything illegal or malicious is carried out by another user then your IP address can be identified by the source. You could be looking at legal action against you.

Do use Tor for anonymous email because your usual email services will not encrypt your messages. Tor on its own will only disguise where you are, so you will need a Tor-enabled email service to run on the browser. Most services have been closed down by law enforcement agencies but consider using ProtonMail. ProtonMail is an end-to-end encrypted email provider. The email provider introduced a Tor hidden service specifically to combat censorship and surveillance of users. A free account will limit your storage space and the number of messages you send per day.

Do not use too many browser add-ons as it will slow it down and compromise your privacy. Tor comes with the best add-ons already installed - NoScript and HTTPS - which is all you really need to stay anonymous.

Do report any illegal activity, especially if it involves child pornography. You

can submit an anonymous report to the Internet Watch Foundation (IWF, report.iwf.org.uk). You can also report to Crimestoppers (Failing to do this could land you in serious trouble if you have stumbled on something deeply unpleasant).

Anonymity against the Government

Governments spy on individuals and companies to prevent crime and terrorist activities. Governments are always passing new laws to increase surveillance giving them greater powers on information they can access. There are some countries like Saudi Arabia that are constantly monitoring people's activity over the net with an oppressive regime. Government bodies in the UK including GCHQ and the Home Office now have the power to force communications companies to keep records of all the websites you visit and the messaging services used over the last 12 months. Government agencies can also hack into your phones, computers and networks and collect and retain confidential data. There are controls on how they use the information but they do not require a warrant, so it is easy for them to access information if they so wish. Encryption is the best way to avoid surveillance so use your VPN to guard your online communications.

You haven't just got to worry about the government hacking into your important data, cyber criminals are another problem. Cyber criminals are after your confidential information for their own financial benefit. Cyber criminals will use a range of techniques to get hold of your personal data in order to use for financial fraud and identity theft. Methods include phishing emails, malware and social engineering. Keylogging is another technique used by criminals to watch everything you type including passwords and personal information such as credit card details. They will use malware to infiltrate your computer enabling them to spy on you to steal the sensitive data. To stop this threat you should not open any suspicious emails or use software from an unknown source. Your anti-virus software should detect whether there any processes recording your key strokes.

Advertisers, internet service providers, search engines and social networks are all spying on you when you surf the net. Advertisers use cookies to track which websites you have visited that is why you will see adverts that are related to something you have looked at. Your ISP can see all of the websites that you have visited and information you have sent via messaging. They can keep records of your activity for a long time and share this with government agencies and the police. Search engines will make a log of every single search you make so they can determine your interests. This in turn helps them to offer better search results and relevant content. The information can also be organised by your location and sites previously visited. Social networks

like Facebook and Twitter will aim to build profiles on their users so they can tailor advertising. Even just clicking the 'like' button is helping the social network understand the sort of posts that you want to see. Tor will help guard against these privacy invaders by making it difficult to track your website visits and blocking cookies through the browser.

As you can see from reading this chapter there are a lot of prying eyes that you need to protect your privacy from. Criminals are probably the biggest worry and the techniques used for cyber security (including the use of Tor) should be focused on blocking cyber hackers.

Resources

Interesting Dark Web sites – that are perfectly legal!

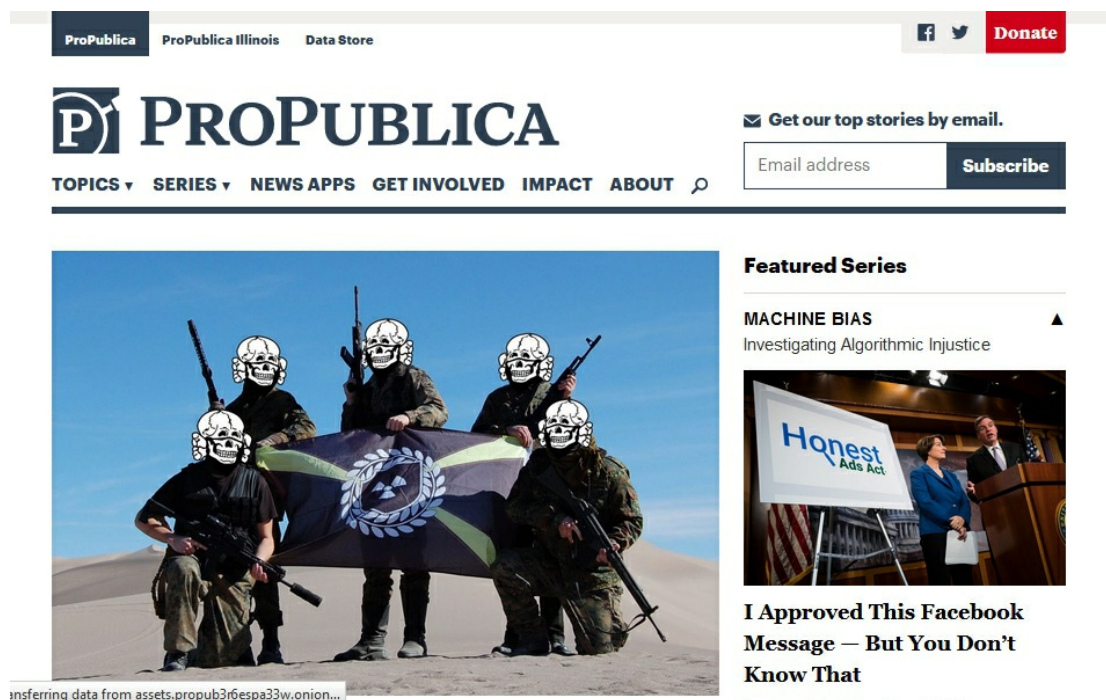
The Dark Web does not just consist of illegal activity; there are many useful sites that are actually legal and informative.

Facebook – www.facebookcorewwwi.onion

The social media network provides a Tor version that is a reliable and secure method of communication for people concerned about surveillance.

ProPublica – www.propub3r6espa33w.onion

ProPublica is a non-profit website that aims to expose a government that has abused its power and betrayed public trust. It is a great site for investigative journalism and allows people in internet-censored countries to read the content through the safety of Tor, without punishment.



Intel Exchange – rrcc5uuudhh4oz3c.onion

This is a must for anyone who is interested in conspiracy theories, cover-ups and leaked documents. The exchange is one of the safest places to view and share information with some amusing threads.

WikiLeaks – wlupld3ptjvsgwqw.onion

A renowned site mostly because of the recent press coverage it has received resulting in WikiLeaks founder, Julian Assange, losing a lot of goodwill. The site still holds a lot of acclaim and has important sources of uncensored political information. If there is anything sinister going on in politics this site sets out to uncover the truth, even at the expense of a court case. You can access the site on any browser but documents have to be submitted through Tor. Files will be encrypted during the upload.

Flashlight – kxojoy6ygju4h6lwn.onion

This site gathers information and news about online privacy, bitcoins and Tor-related projects. The site is a constantly updated news feed along with a forum for discussion.

The screenshot shows the Flashlight website. At the top is the logo "FLASHLIGHT" with the tagline "AN INFO BEAM IN THE DARKWEB". Below this is a navigation bar with links: HOME, NEWS, LINKS, USEFUL ARTICLES, FREE BITCOINS, FLASHCHAT (highlighted in green), Q&A, HIDDEN CLUB, FORUM, and CONTACT. A large banner below the navigation bar reads "DECENTRALIZED PLATFORM FOR HONEST TESTIMONIALS" and "Join Us To Make TOR Better". It also includes a "HIDDEN REVIEWS" section with the URL "http://xrwwait2nw6etj4b.onion". The main content area features two articles. The first article is titled "It's Not Easy To Put a Diaper on a Capuchin Monkey" and is posted by Fusion on February 22, 2018. The second article is titled "Turkey is also planning a state cryptocurrency Turkcoin" and is posted by TheBitcoinNews on February 23, 2018. To the right of the articles is a "Verified by" section with logos for The Hidden Wiki, AHMA.FI, and DEEP DOT WEB. At the bottom right, there is a blue banner that says "POWERED WITH BLOCHCHAIN".

Tor Project

Use this site to download Tor and get support
<https://www.torproject.org/>

Virtual Private Networks

ProtonVPN - <https://protonvpn.com/>
Windscribe - <https://windscribe.com/>

Anonymous Email Providers

ProtonMail - <https://protonmail.com/> or protonirockerxow.onion for Tor
Bitmessage - <https://bitmessage.org/> or bitmailendavbec.onion for Tor

Bitcoin Wallets

Use one of these wallets to securely store your cryptocurrency

Green Address - <https://greenaddress.it/en/>
Blockchain - <https://www.blockchain.com/> or blockchainbdgpzk.onion for Tor

Disposable Email Service

Nada - <https://getnada.com/>
Fake Name Generator - <https://www.fakenamegenerator.com/>

Magazines and Websites

WebUser – UK magazine published fortnightly with excellent tips on staying anonymous online.

DeepDotWeb - <https://www.deepdotweb.com/>
Lots of interesting articles and new stories linked with the Dark Web