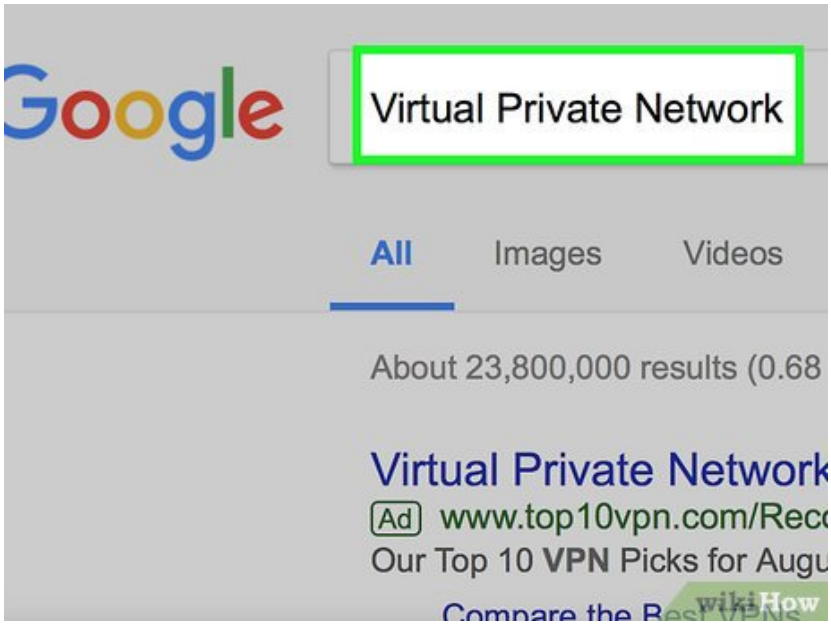
How to Maintain Your Privacy Online

This wikiHow teaches you how to minimize your online footprint by using encrypted services and hiding your online activity from your Internet Service Providers and ad companies alike. While you can never guarantee privacy on the Internet,...

Part 1 of 4:

Finding a Virtual Private Network (VPN)

1. 

Search for a VPN online. VPNs route your browser traffic through a server other than your local one, which makes it impossible for your Internet Service Provider (ISP) to see your browsing history. Things to look for in a VPN include the following:

1. **On an HTTPS site** - Never download browser security software from a site whose URL doesn't begin in "https"; unencrypted (non-HTTPS) sites make it easy for other people to steal your information.
2. **Based outside of the United States** - VPN servers based outside of the United States aren't subject to US guidelines, meaning they can't be forced to expose users in the event of an investigation.
3. **Multiple-device support** - Protecting your computer won't do anything for your mobile phone or tablet. Find a VPN that has an iOS and/or Android extension as well to stay protected across all of your devices.

EXPERT TIP

Picture 2 of How to Maintain Your Privacy Online

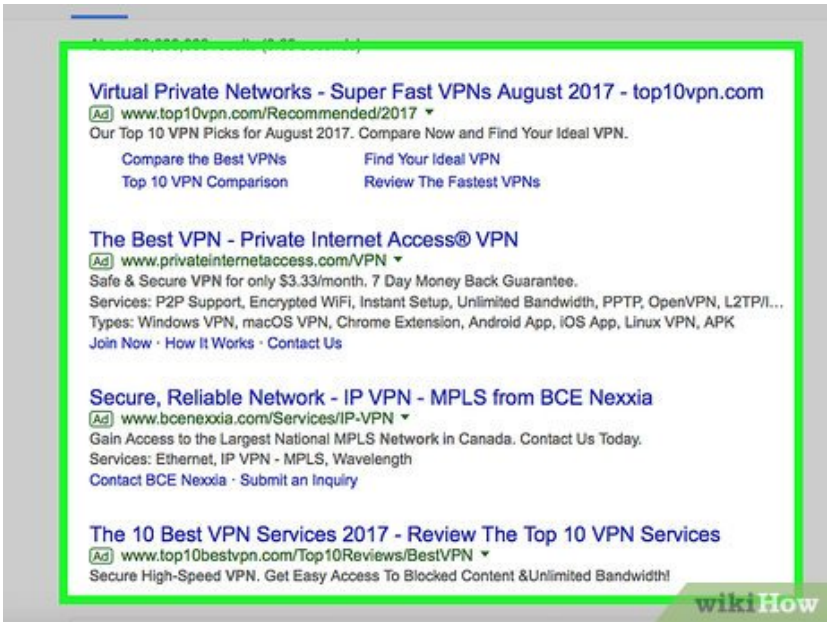
Spike Baron
Network Engineer & Desktop Support

Spike Baron is the Owner of Spike's Computer Repair based in Los Angeles, California. With over 25 years of working experience in the tech industry, Spike specializes in PC and Mac computer repair, used computer sales, virus removal, data recovery, and hardware and software upgrades. He has his CompTIA A+ certification for computer service technicians and is a Microsoft Certified Solutions Expert.

Picture 3 of How to Maintain Your Privacy Online

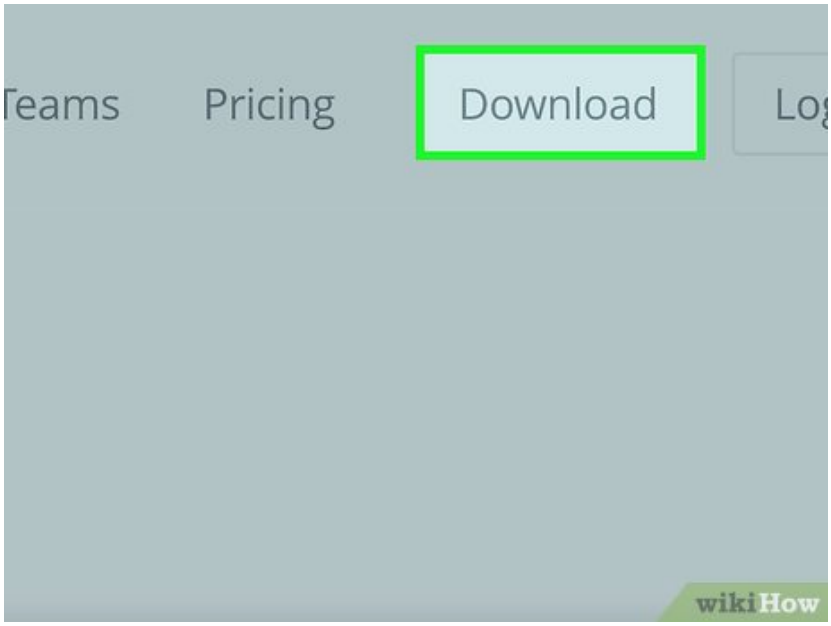
Spike Baron
Network Engineer & Desktop Support

Our Expert Agrees: "A VPN masks your IP address from the world while you're online. No one will know where you're coming from and it's a great way to browse the internet safer. You should also avoid sharing too much data and clicking on attachments from strangers."

2. 

Compare your options. Keep in mind that, when it comes to sponsored content, you may not get an honest review for a paid spot in a list. Some things you might compare are ratings across multiple sites, performance, overall security, and price.

1. You can find trustworthy VPN comparisons on https://thatoneprivacysite.net/simple-vpn-comparison-chart/ and on https://privacytoolsio.github.io/privacytools.io/#vpn/.
2. For specific VPNs, try AirVPN (https://airvpn.org/) and BlackVPN (https://www.blackvpn.com/).

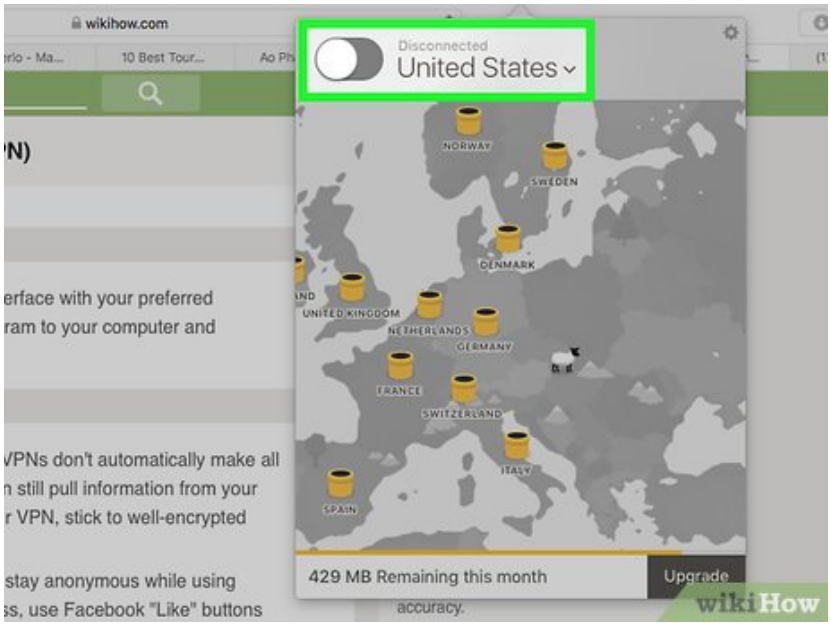
3. 

Download your selected VPN from its official site. Some sites, such as CNET, will provide download mirrors for sponsored or preferred software. Unless there is no other place to download the VPN and you're positive of the download link's validity, refrain from downloading your VPN from anywhere but the official site.

1. Again, if the site isn't HTTPS-encrypted, don't download a VPN from it.
2. Most VPNs are paid options, so you'll likely need to pay before downloading. Consider using PayPal to pay instead of a credit or debit card.

4. 

Install your VPN if needed. Some VPNs simply interface with your preferred browser, while others necessitate installing the program to your computer and activating it before browsing.

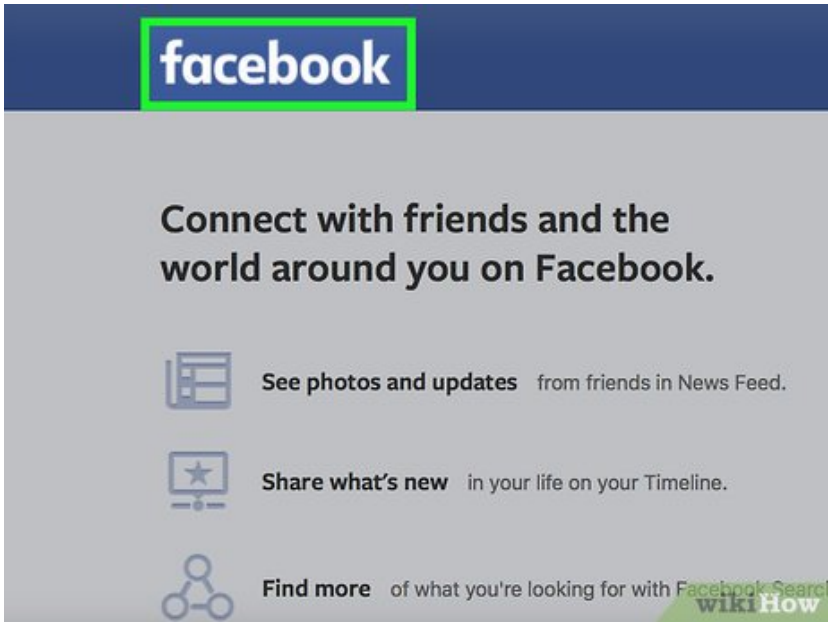
5. 

Use your VPN in conjunction with HTTPS sites. VPNs don't automatically make all of your browsing private, since non-HTTPS sites can still pull information from your browser and publicly display it. To get the most out of your VPN, stick to well-encrypted sites and refrain from giving out your information.

1. Half of the privacy battle comes from choosing to stay anonymous while using encrypted services. If you enter your email address, use Facebook "Like" buttons on other sites, or perform other identifying actions, your VPN won't necessarily prevent that information from being viewed by other people.

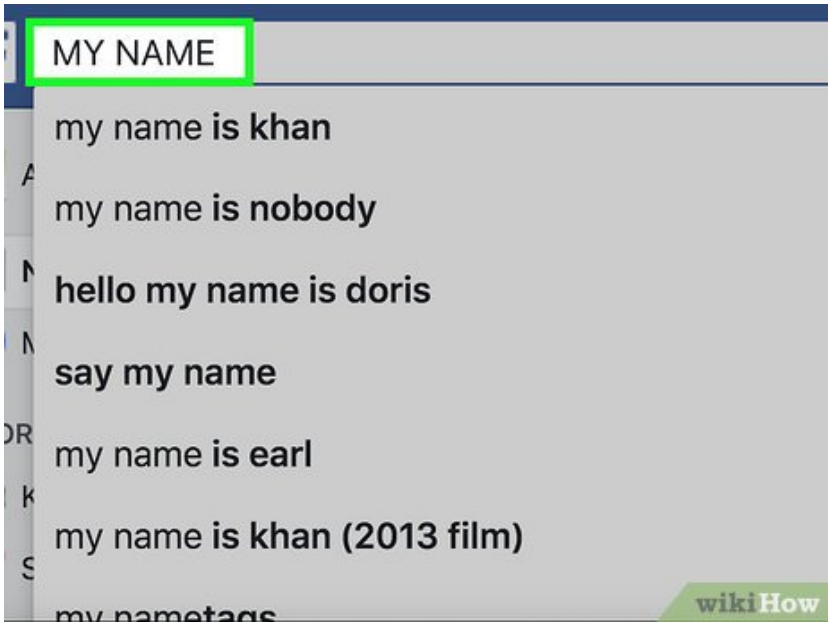
Part 2 of 4:

Using Social Networks

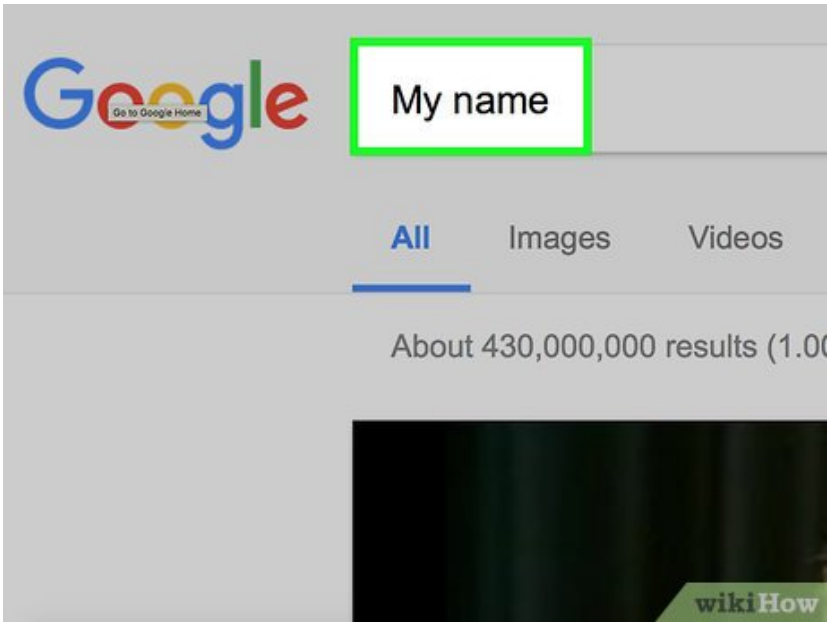
1. 

Make your social media accounts as private as possible. Most social networks will allow you to customize your privacy settings. These settings dictate how others can search for you, and what information is available for the public to view. Most social networks have default settings that allow a lot of information through, so it is up to you to change the settings to increase your privacy.

1. To make Facebook private, click the downward-facing arrow in the top-right corner of the page and select **Settings**, then click **Privacy**. Here you can set who can see your posts, how people can look you up, and if you want search engines to show your profile. If you want to stay as private as possible, limit everything to just your Friends, and then remove any friends from your list that you don't want to share with.
2. On Twitter, your tweets are public by default, and anyone can see them. You can change this to "Protected" mode in the Twitter settings menu; protected tweets cannot be retweeted or viewed by people you haven't approved, and they will not show up in Google searches.[1]
3. In Google+, your privacy settings are the same as those for all of your Google accounts. To manage your privacy options, click your picture in the top-right corner, and then select **Account**. In the left menu of the Account page, select **Privacy**. Here you can adjust what information can be seen by whom. Anything marked "Public" can be seen by anyone that searches for you. You can change your settings so that only the people that you designate can see specific information.

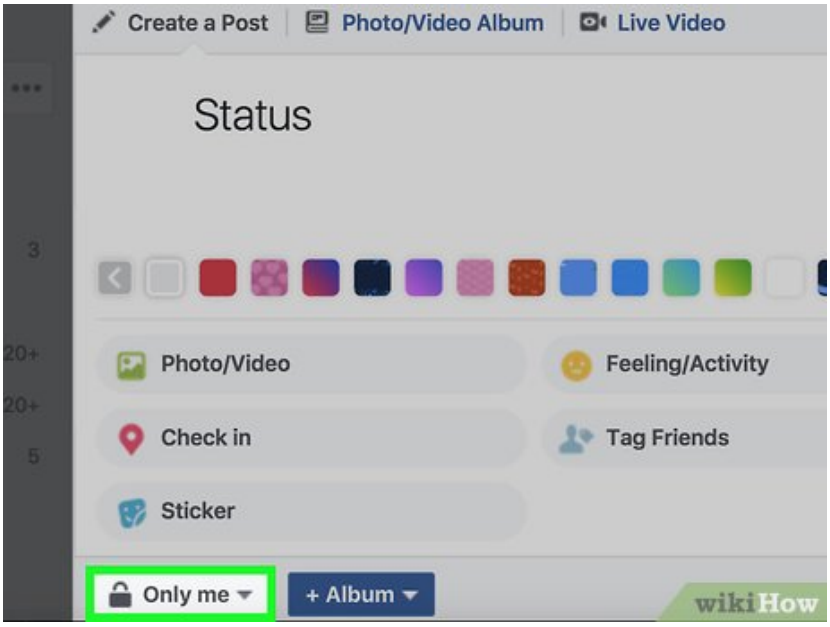
2. 

View your profile as a random person. Sign out of your social network site, and then search for yourself on that site. Browse your profile and ensure that there isn't any data on there that you don't want publicly accessible. If you find information that you want hidden, enter your profile and either remove it or set it to hidden.

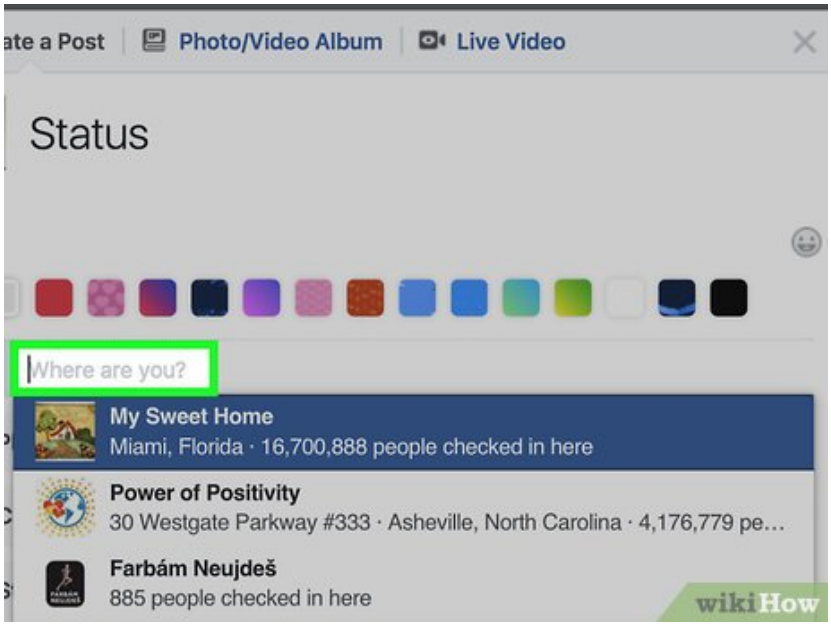
3. 

Do a web search for yourself. Use any popular search engine to search your own name. Take note of what appears, and then do what you can to remove this information. For example, if a web search shows your profile for a high school reunion site, contact that specific site to remove your information.

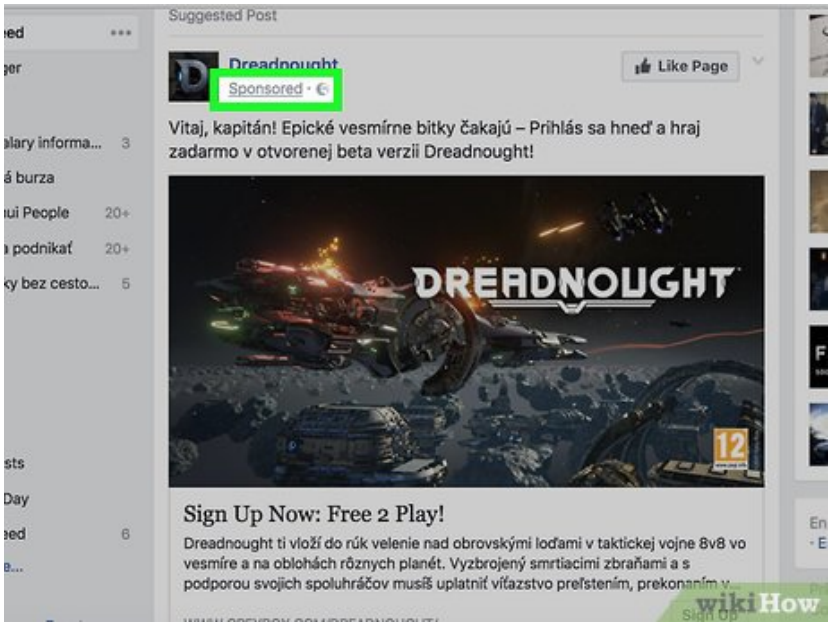
1. If you have unused accounts on old sites, go back and delete them to remove your information from that site's database.

4. 

Limit the information you share. Even if you set everything to private, the companies that run the social networks still have access to all of your information. By limiting the amount of information you share, you'll limit the amount of knowledge these companies have about you.

5. 

Disable location-based posting. Many social networks, such as Facebook, allow you to include the location you are at when you make a post. These locations are then saved to a database. Avoid sharing your location unless it is critical to your post that you share where you are.

6. 

Understand that social networks make money off of advertising. By signing up for a social network, you are already compromising your privacy, even if you never post. Facebook can track your web use through the Like system, and Google does similar things with their +1 system. Even if all of your settings are set to Private, these companies will still use your information to attempt to sell you things.

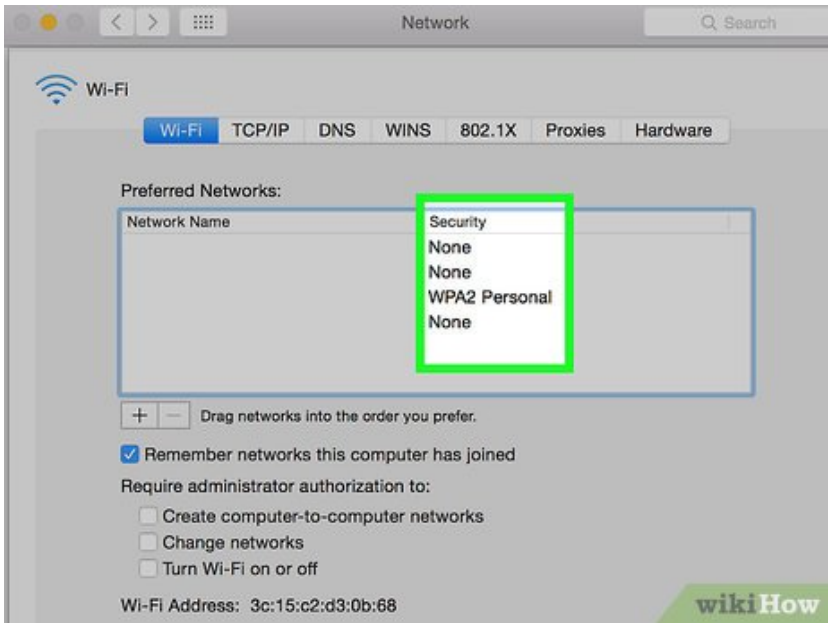
Part 3 of 4:

Browsing

1. 

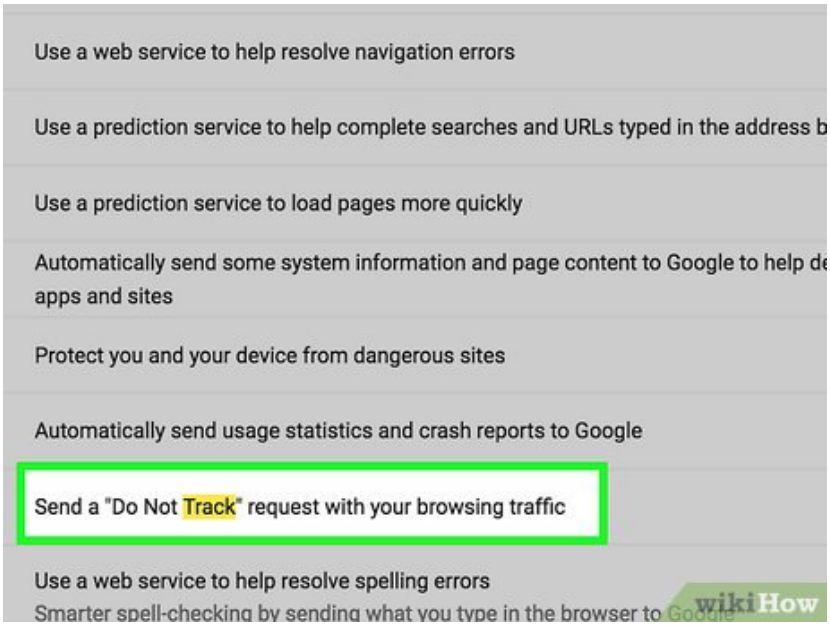
Use a secure web browser. Internet Explorer comes bundled with all versions of Windows, but the browser is more susceptible to attack than browsers such as Firefox and Chrome. These browsers are available for free, so consider switching to help protect yourself from viruses and malware.[2]

1. You should avoid using browsers like Tor or I2P since these sites are predominately used for illicit activity, and the simple act of using one may draw unwanted attention to you.[3]
2. In general, stay off of the dark web when attempting to skirt surveillance. Unless you're extremely careful and well-experienced in navigating the dark web, you're likely to run into malware or worse.

2. 

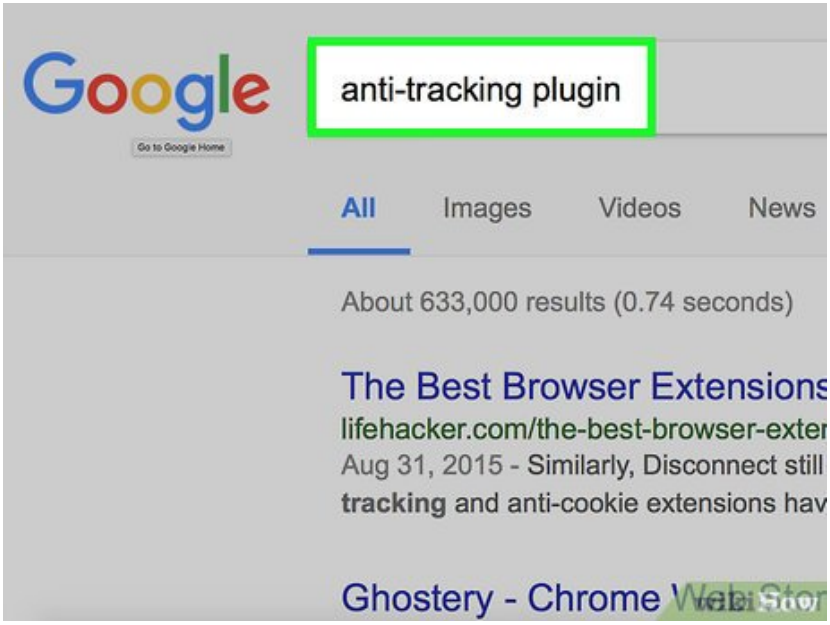
Avoid using unsecured networks. Wi-Fi networks that don't require a password--or even networks that do require a password but accommodate several people at once (e.g., an airport or a coffee shop)--put you at increased risk of having your data stolen.

1. If you must use an unsecured network, refrain from logging into social media, bank accounts, or other sensitive places.

3. 

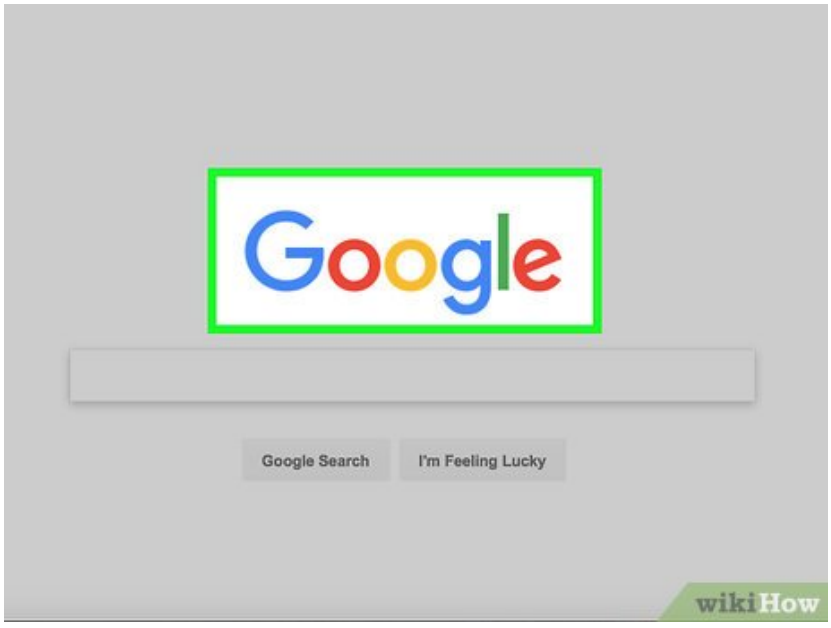
Send a Do Not Track request. Websites can choose whether or not to honor this request, but in general it will lower the number of websites that track your actions online. You can turn this on in most browsers ion the Advanced section of the Settings menu.

1. Do not assume that by selecting this you will no longer be tracked. Many websites will still collect your browsing information.

4. 

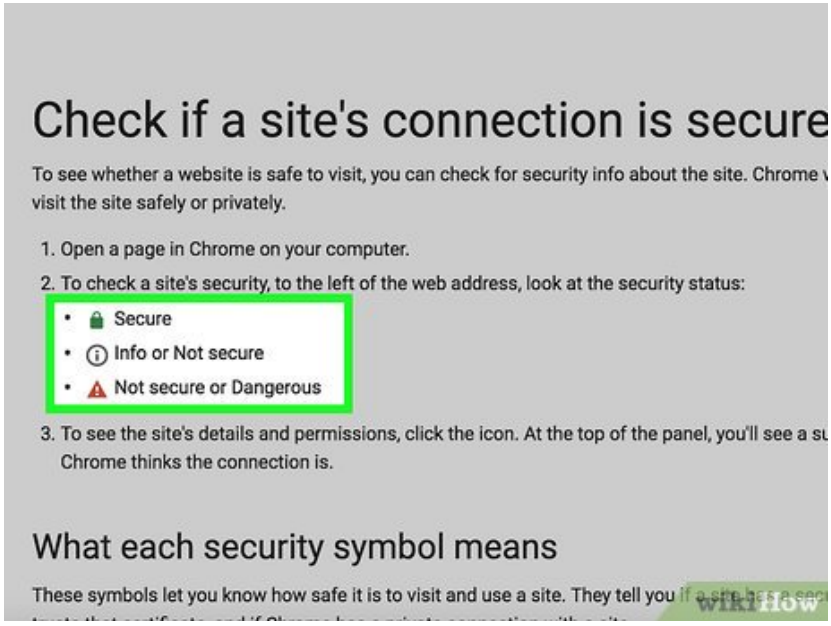
Install an anti-tracking plugin. These plugins are typically much more effective than simply enabling Do Not Track, and they can be installed for free. One of the most popular plugins is DoNotTrackMe from Abine.

1. uBlock Origin, which can be found in the Chrome, Firefox, and Opera app stores, is a well-reviewed app that blocks all ads in addition to attempts to access your IP address from third-parties and your ISP.

5. 

Avoid major web services. Programs such as Skype and web services such as Google Search have recently been shown to be compromised by US government surveillance. To protect your web browsing and messaging, switch to programs that aren't located in the US, so that they do not fall under the jurisdiction of US law.

1. Popular secure searching alternatives include Startpage (https://www.startpage.com/), DuckDuckGo (https://duckduckgo.com/), and Ixquick (https://www.ixquick.eu/).
2. Popular messaging alternatives include: Jitsi (https://jitsi.org/), Pidgin (https://pidgin.im/), and Adium (https://adium.im/).

6. 

Only provide personal information on sites protected by HTTPS. This is the secure form of the standard HTTP address, and data transferred to and from HTTPS websites is encrypted. Most secure sites will automatically load the HTTPS version of their website when you visit, but you can force it to load on all supported websites by using a browser plugin such as HTTPS Everywhere (https://www.eff.org/https-

everywhere) for Firefox.

1. If a site doesn't support HTTPS, then there is nothing that you can do to force an HTTPS connection. Avoid entering any personal information into these sites.
2. You can identify a secure site by looking for the Secure indicator in your web browser. Each browser shows it a little differently, but in general you should see a lock icon or the word "Secure" next to the address of the site you are visiting. You should also be able to see 'https' at the beginning of the address.

7. 

Connect to a proxy server. A proxy acts as a middleman between you and the internet. Requests are sent from your computer to the proxy, and then from the proxy to the internet. Results are returned in the opposite direction. This has the effect of masking your computer, as websites will think the proxy server is the one that is requesting the information.

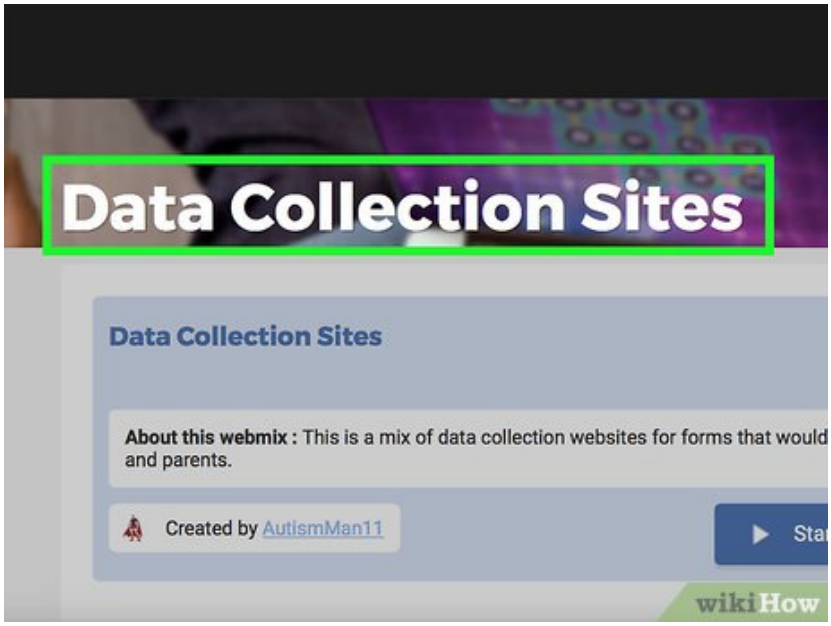
1. If you connect to the proxy through a VPN, then all of the data that is sent between your machine and the proxy is encrypted.

8. 

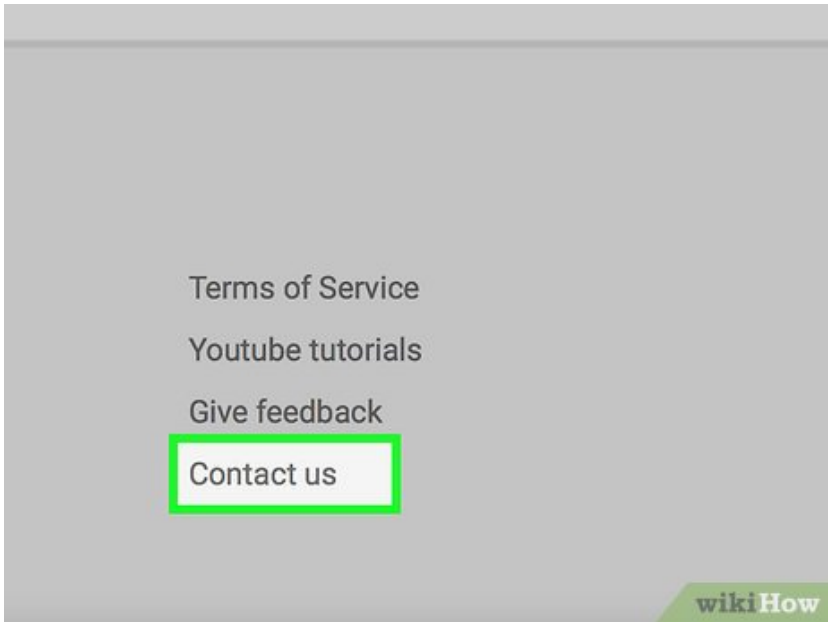
Encrypt your emails. You can use GPG (a free encryption solution) to exchange encrypted email messages. GPG is end-to-end encryption that requires both the recipient and the sender have created and exchanged their GPG Public Keys. You can use GPG on Windows or on Linux.

Part 4 of 4:

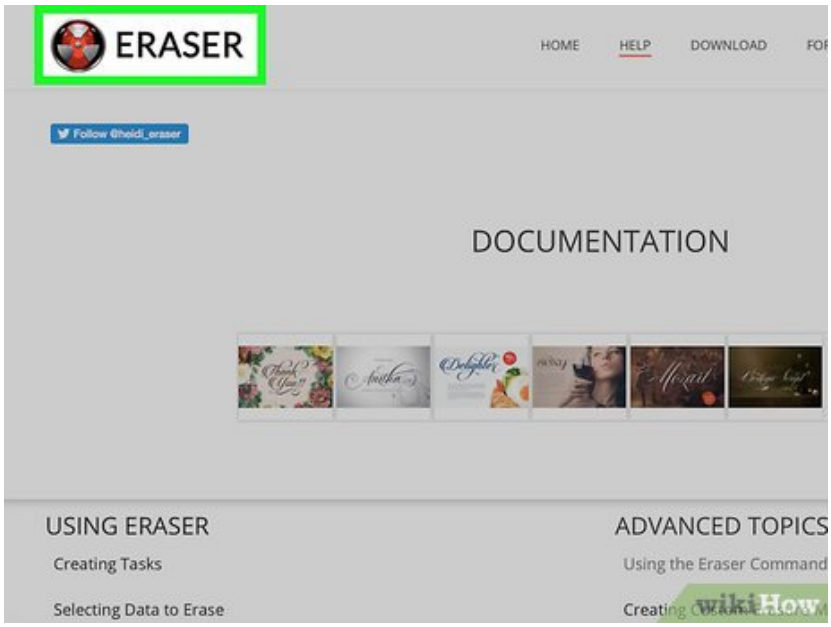
Controlling Personal Information

1. 

Find a list of data collection sites. There are multiple companies online that exist solely to collect data on you and then sell it to marketers. These sites take public records, social network information, browsing information, and more to create a profile about you that they can sell. Opting out of these lists can be time consuming and difficult.

2. 

Remove yourself from the lists. Several sites have lists of the companies that collect data, as well as information on how to remove yourself. This typically involves emailing and calling the company until you reach someone who can delete your information. This can be a very time-consuming and frustrating process, as many of these companies purposefully make it difficult to remove yourself.

3. 

Pay to have your data deleted automatically. There are services available that will delete your records from listing sites. These services essentially perform the same functions that you can do for free, but take care of it for you so that you don't have to spend your time trying to track down sites and people to talk to.

1. These services are often subscription based. This is because even if you remove yourself from a list, you will often be placed back on it after a few months. These services repeat the deletion process every few months to ensure that you stay off the lists.

tips and guides. Thank you for reading and for following us regularly.