Secure Online Browsing

✓ You learned how browsers can leak personal identifying information about you and your machine.

✓ How to configure your browser to become more private in addition and offer advice and tools to conceal your real digital fingerprint.

✓ There are many desktop browsers; the market share is mainly divided between Microsoft Internet Explorer (IE), Mozilla Firefox, Safari, Opera, and Google Chrome.

✓ IE and its successor Edge come preinstalled on the Windows OS; however, we always encourage users to use open source software to assure maximum security when working online.

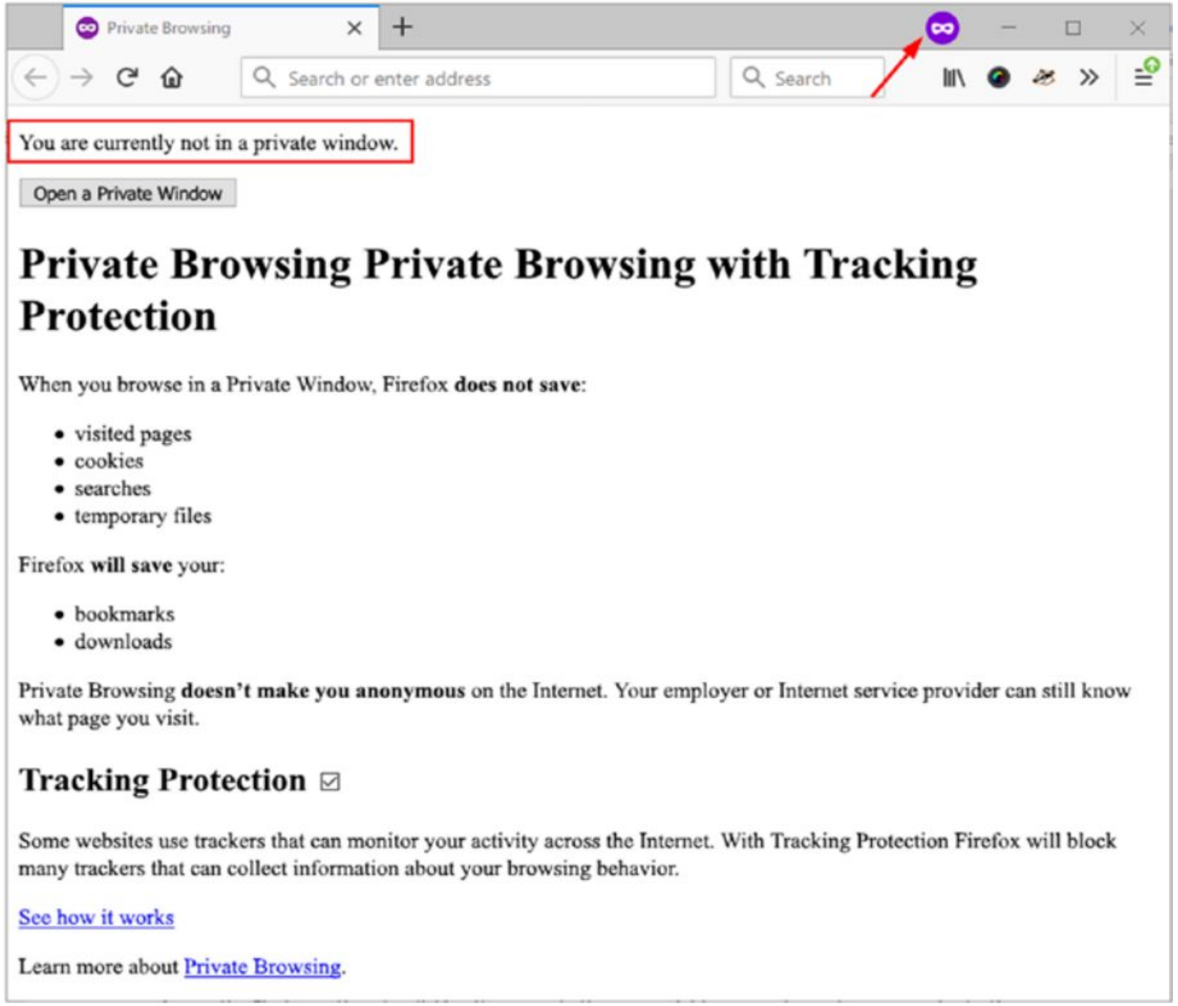
✓ Mozilla Firefox is still considered the only true open source browser of the main browsers mentioned.

✓ The Epic browser is developed by a group called Hidden Reflex and promotes privacy worldwide; this browser is based on Chromium (like Google’s Chrome browser) and comes with enhanced security features to eliminate online tracking.

✓ It also comes with a free built-in VPN to conceal your IP address and protect your online communications. You can give it try at https://epicbrowser.com/index.html.

Configuring Firefox to Become More Private

- ✓ Basic tips to secure your online browsing when using Firefox.
- ✓ Turning on Private Browsing- when you enable private browsing in Firefox, the browser will not record your visited pages, cookies, temporary files, and searches.
- ✓ Firefox will also activate tracking protection, which will block online trackers from monitoring your browsing history across multiple websites.
- ✓ To enable private browsing in Firefox, open the Firefox browser, and press Ctrl+Shift+ P. A new private browsing window will appear, as shown in the figure on right.



You are currently not in a private window.

Open a Private Window

Private Browsing Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- cookies
- searches
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.

Tracking Protection ☑

Some websites use trackers that can monitor your activity across the Internet. With Tracking Protection Firefox will block many trackers that can collect information about your browsing behavior.

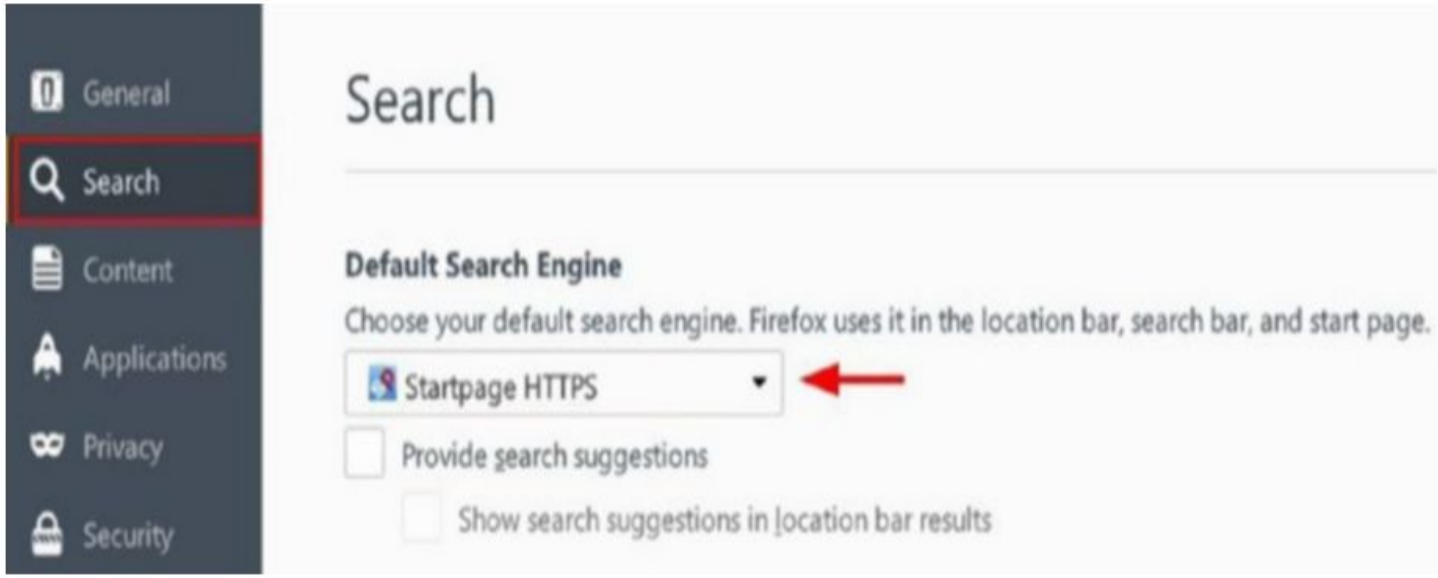
See how it works

Learn more about Private Browsing.

A new private session window opened in the Firefox browser

Changing the Firefox Settings to Become More Private

- ✓ There are many tweaks to make your Firefox browser more private.
- ✓ Access the Firefox options by clicking the menu in the upper-right corner of your browser and selecting Options, see figure on right



Search

Default Search Engine

Choose your default search engine. Firefox uses it in the location bar, search bar, and start page.

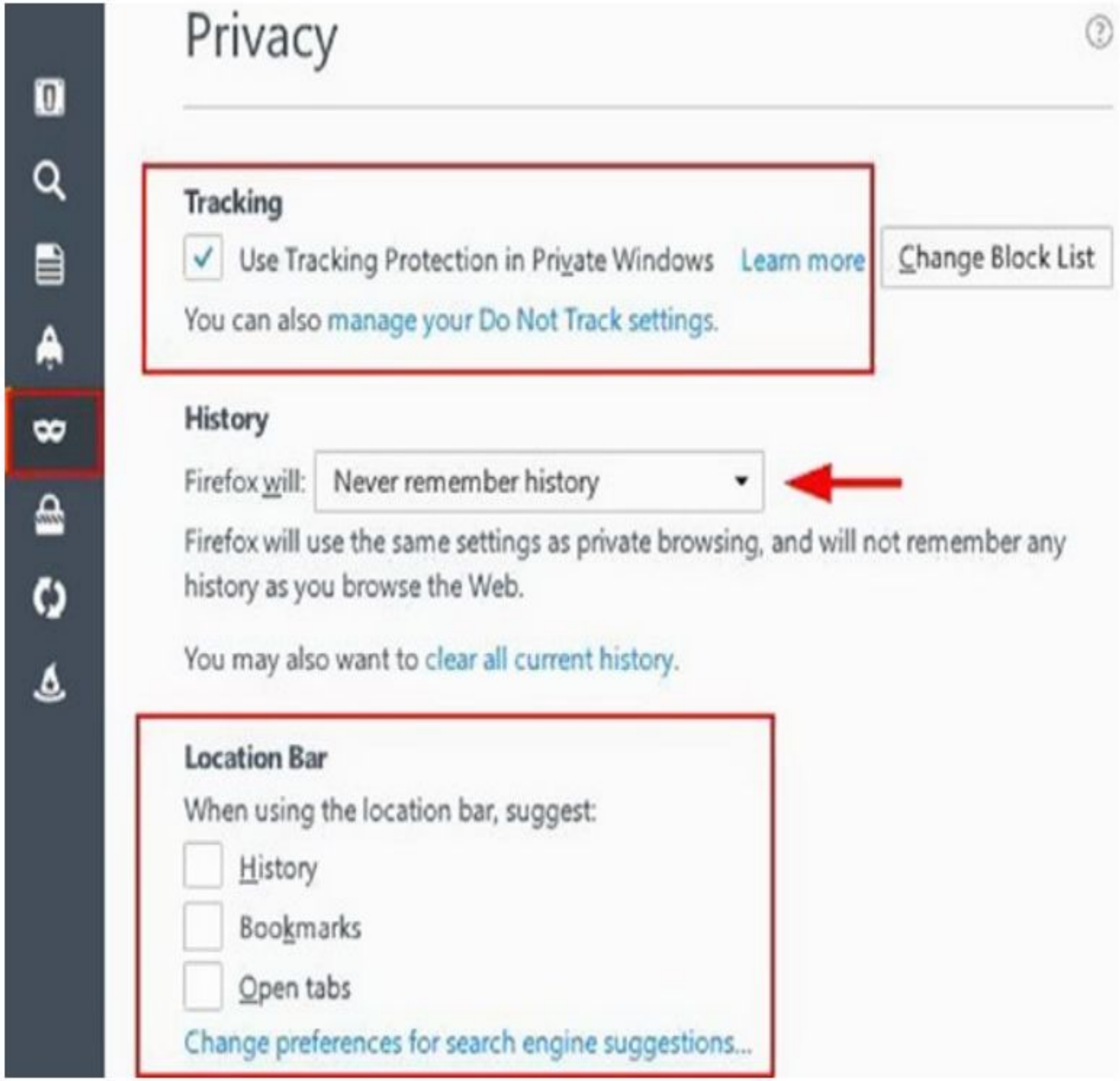
Startpage HTTPS

□ Provide search suggestions

□ Show search suggestions in location bar results

Use an anonymous secure search engine that does not track your online activities

- ✓ Move to the Privacy tab.
- ✓ You need to turn on the option Use Tracking Protection in Private Windows.
- ✓ Now, go to the History section on the same page and select the option “Never remember history” so that Firefox will delete all your history every time you close it.
- ✓ Finally, go to the Location Bar section and disable all the suggestions in the search bar because the suggestion process can leak excessive data about you.
- ✓ Your Privacy tab should look like, as shown in figure on right.



Privacy

Tracking

☑ Use Tracking Protection in Private Windows Learn more

Change Block List

You can also manage your Do Not Track settings.

History

Firefox will: Never remember history ▾

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

Location Bar

When using the location bar, suggest:

☐ History

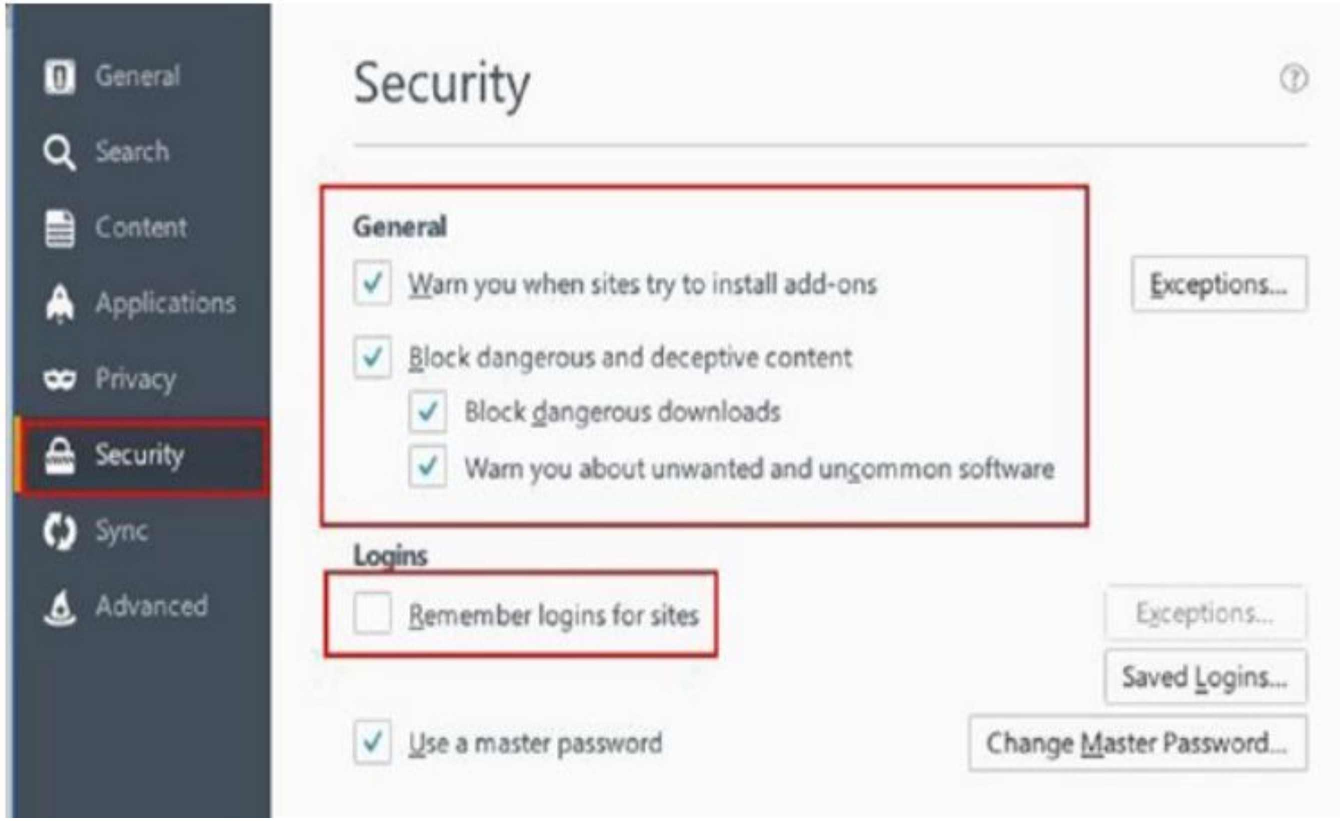
☐ Bookmarks

☐ Open tabs

Change preferences for search engine suggestions...

Configuring the Privacy tab in the Firefox browser for better privacy

- ✔ Move to the Security tab and configure it like, as shown in figure on right.
- ✔ Go to “Privacy & Security” tab ➤ “Firefox Data Collection and Use” pane and disable the following options:-
  - ✔ Allow Firefox to send technical and interaction data to Mozilla and Allow Firefox to send backlogged crash reports on your behalf.
  - ✔ We are using for this step Firefox Quantum edition—version number 61. Crash reports can contain valuable data about your computer status that can make you vulnerable if it falls into the wrong hands, so it is better to disable them.



Security

General

☑ Warn you when sites try to install add-ons

☑ Block dangerous and deceptive content

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Logins

□ Remember logins for sites

☑ Use a master password

✔ While you are still on the Advanced tab, go to the Network subtab, and make sure that the option “Tell me when a website asks to store data for offline use” is selected.

✔ This prevents websites from planting a tracking code on your computer.

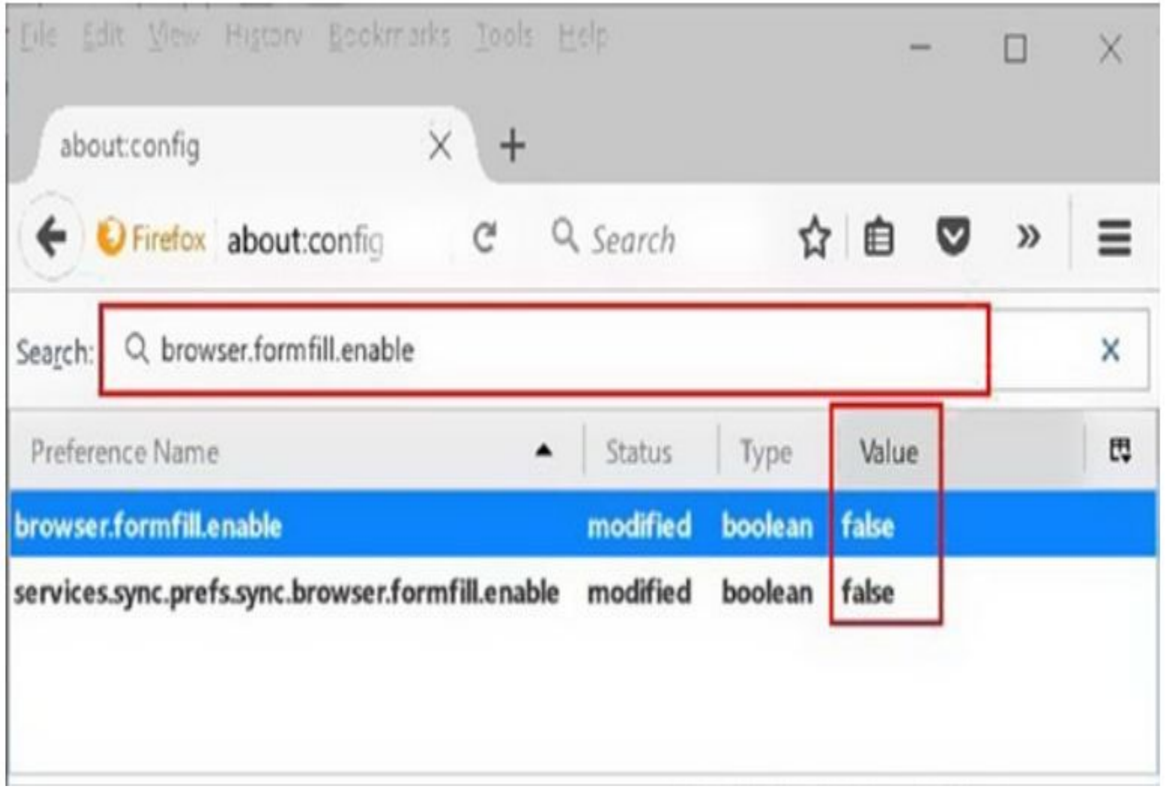
✔ Now that you have finished configuring the basic settings of Firefox to make it more privacy-friendly, you need to move to the advanced settings to continue your work.

✔ Access the Firefox advanced settings page by typing about:config in the URL address bar of your browser.

✔ A warning message will appear; hit the button “I accept the risk!” to access the advanced settings panel.

✔ To access a specific setting, you need to type its name in the Search box that appears at the top of the page. To begin, let’s change the first setting named browser.formfill. enable to false (double-click to change the settings value).

✔ This forces Firefox to forget form information, as shown in figure on right.



Search: browser.formfill.enable

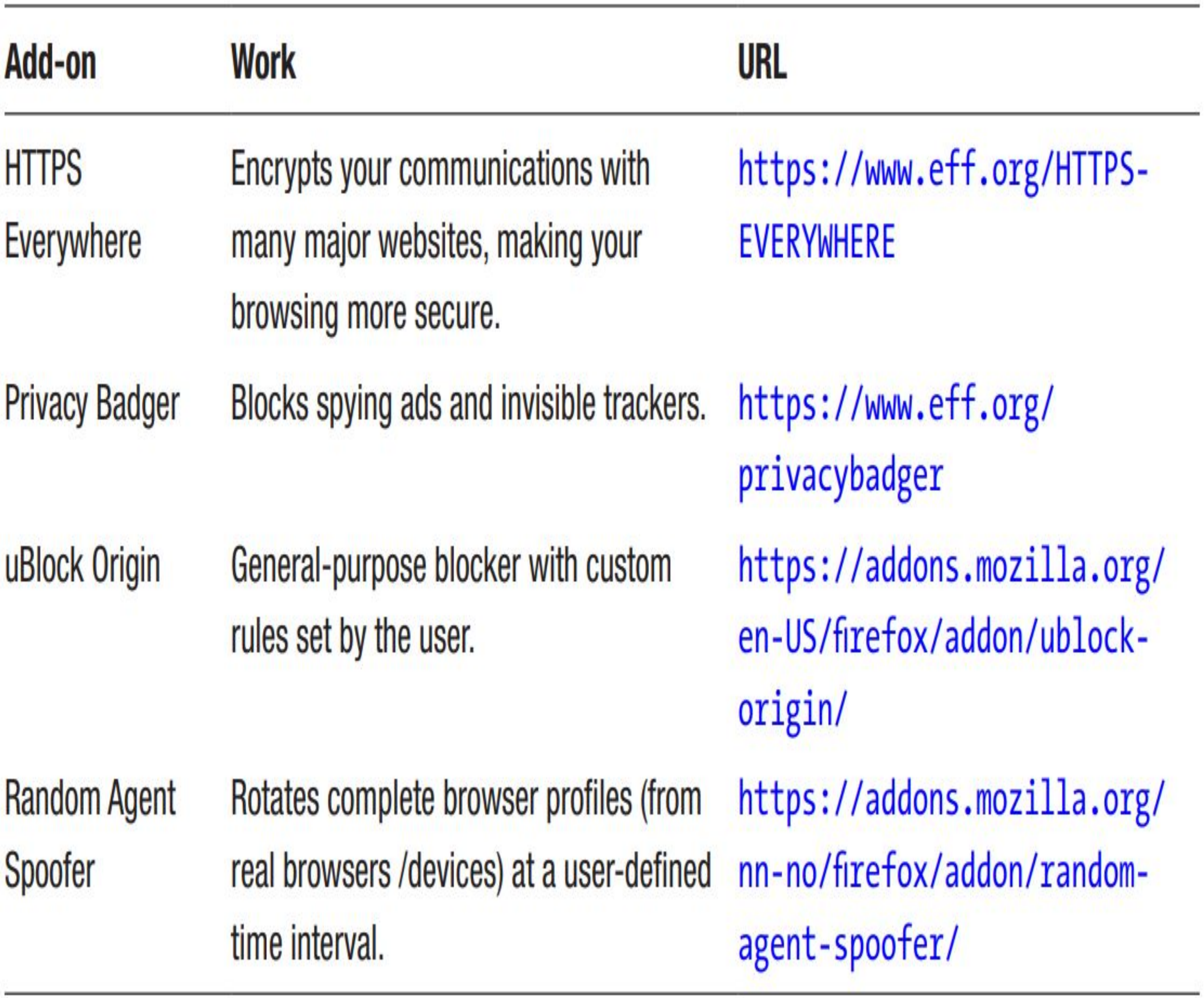
Preference Name	Status	Type	Value
browser.formfill.enable	modified	boolean	false
services.sync.prefs.sync.browser.formfill.enable	modified	boolean	false

✔ Accessing the advanced settings page in Firefox and disabling form history in Firefox

- Now, in the same way, you need to change the following settings:-
  - Change browser.cache.disk.enable to false.
  - Change browser.cache.disk_cache_ssl to false.
  - Change browser.cache.offline.enable to false.
  - Change dom.event.clipboardevents.enabled to false.
  - Change geo.enabled to false.
  - Change network.cookie.lifetimePolicys value to 2.
  - Change plugin.scan.plid.all to false.
- These advanced configurations will “harden” Firefox and make it more difficult for outside parties to track your activities.

Firefox Privacy Extensions

- ✓ A selection of the best Firefox extensions that help you to maintain your online privacy is mentioned in the table on right.
- ✓ Please note that some add-on providers may fool users and collect private data about browsing habits and even personal information without their consent, so it is advisable to avoid installing any add-on blindly.
- ✓ Also, if a new reliable add-on appears later (say after publishing this book), ensure that it comes from a reputable trusted developer and install it from https://addons.mozilla.org exclusively.



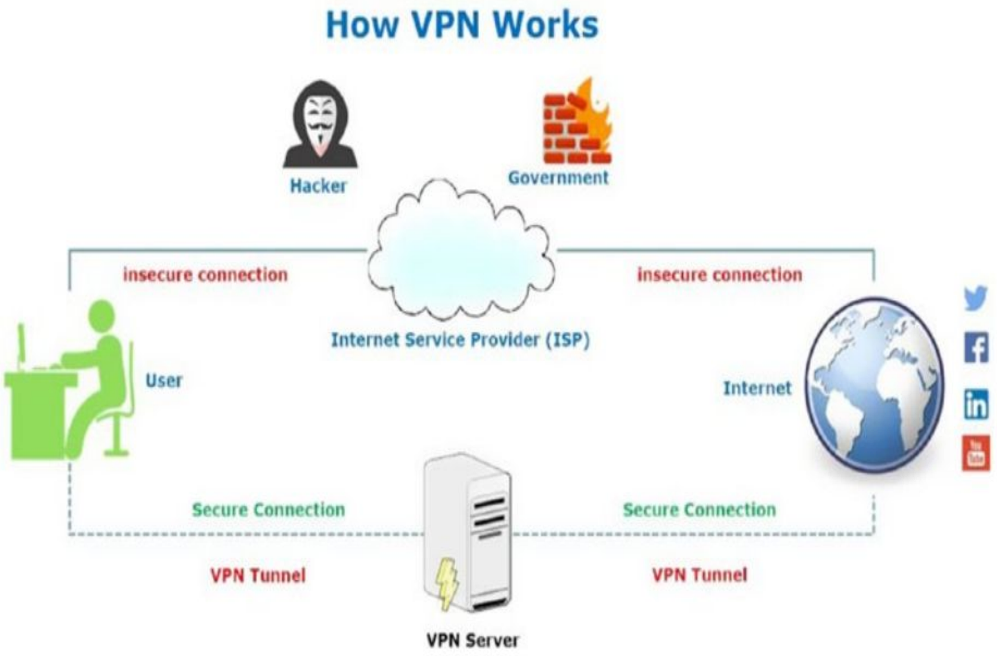
Add-on	Work	URL
HTTPS Everywhere	Encrypts your communications with many major websites, making your browsing more secure.	https://www.eff.org/HTTPS-EVERYWHERE
Privacy Badger	Blocks spying ads and invisible trackers.	https://www.eff.org/privacybadger
uBlock Origin	General-purpose blocker with custom rules set by the user.	https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
Random Agent Spoofer	Rotates complete browser profiles (from real browsers /devices) at a user-defined time interval.	https://addons.mozilla.org/nn-no/firefox/addon/random-agent-spoofer/

Secure Online Communication

- ✔ How to use different techniques to conceal your real IP address and to make your connection encrypted so it is hard to intercept.
- ✔ VPN and proxy servers will help to mask your traffic; outside observers will see that there is traffic originating from your computer, but they cannot see what is passing (for example, ISPs and governments cannot see which websites you are visiting).
- ✔ In anonymity, an outside observer should not be able to know the source of the connection; hence, they cannot attribute your online activities to you. Both privacy and anonymity are important for any OSINT analyst and should be fully understood before you begin your OSINT work in the rest of the book.

VPN

- ✔ A VPN allows a user to establish a secure connection from one site to another across the Internet.
- ✔ It is widely used in corporations to access remote sites while assuring the confidentiality of sensitive data.
- ✔ The VPN also gives users anonymous IP addresses, making them appear as if in another location so they can avoid censorship, share files with other people privately, and more.
- ✔ Nowadays a VPN is a necessity for anyone who cares about their privacy when going online.

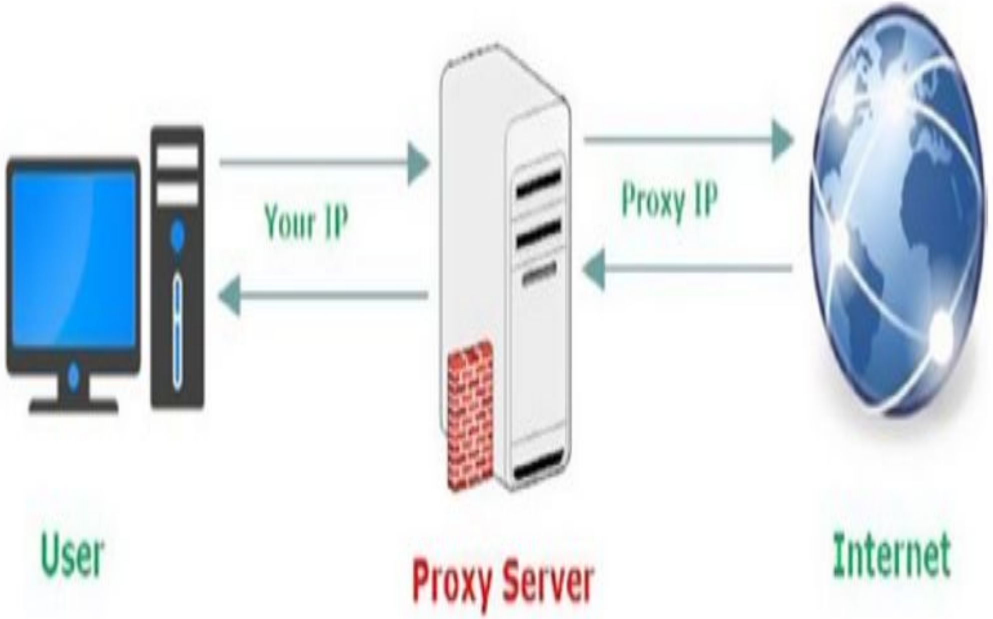


How a VPN works (source: www.DarknessGate.com)

- ✔ VPN vendors offer varying features. You should care about the following features when selecting your VPN provider:-
  - ✔ Do not subscribe to VPN service providers that are based in one of the following countries: United States, United Kingdom, Australia, New Zealand, Canada, Denmark, France, Netherlands, Norway, Belgium, Germany, Italy, Spain, Israel, Sweden, and of course countries such as Russia, China, Iran, and all Arab states.
  - ✔ The best providers are based in Switzerland and follow its jurisdiction.
  - ✔ A VPN provider must have its own DNS server; it must also support DNS leak protection (more on this next).
  - ✔ It is preferred that the VPN software support the OpenVPN software. This is an open source program that can be audited by anyone to assure it’s vacant from any backdoors.
  - ✔ It should accept anonymous payments such as bitcoin, gift cards, debit cards, and cash.
  - ✔ It is better to support multiple devices at the same time so you can protect your tablet and smartphone data in addition to your laptop or PC.
  - ✔ It should not require many details to set up; a username and a password should be enough.
  - ✔ If your ultimate purpose is anonymity and plausible deniability, use the Tor Browser instead of a VPN.

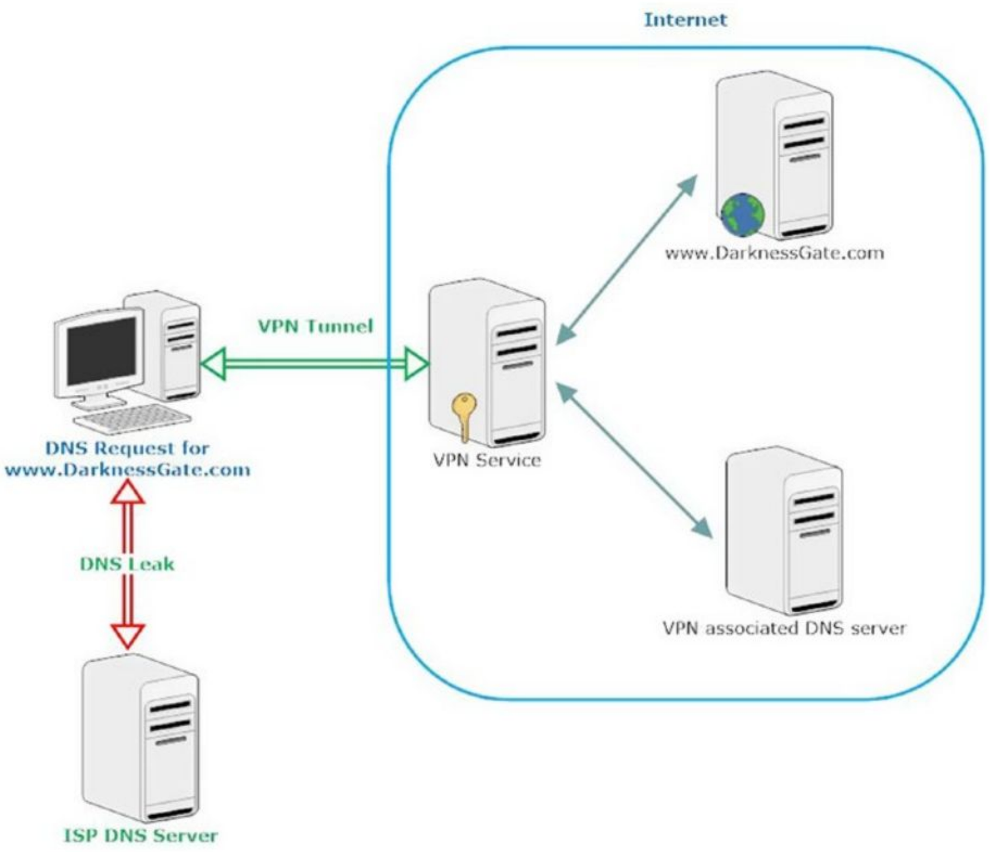
Proxies

- ✓ A proxy server is an intermediary computer that sits between your computing device and the Internet.
- ✓ Corporations use proxies to filter content and to offer a level of security by separating a corporate local network from the Internet.
- ✓ There are different kinds of proxies; the main type is the web proxy that most Internet users mean when using the term proxy.
- ✓ Its main function is to fetch online resources—whether it is a page or a file— from the Internet and then send them to your computer. They also provide anonymity by changing the real IP address of the user's computer into the IP address of the proxy server, see figure on the right.
- ✓ Numerous free proxy servers are available online. However, such services should not be used blindly.
- ✓ A free proxy usually shows advertisements in your browser, which may introduce malicious software or other tracking scripts that could infect or compromise your machine if you click a malicious link.
- ✓ In addition, most free proxies are not secure enough to trust to process and communicate your critical data, such as credit card details and account passwords.



DNS Leak

- ✓ Test Using a VPN—and other anonymity services—does not guarantee that your web browsing history will not get revealed.
- ✓ Sometimes even though you are protecting your connection using a VPN, a connection leak can occur and reveal the real IP address without you being aware.
- ✓ Such a leak occurs when part of your computing device traffic (DNS traffic) is not routed through the secure channel of the anonymity service you are using and hence the VPN.
- ✓ Instead, it gets directed to your ISP's Internet servers (see Figure on right), allowing them to potentially monitor and log the complete web browsing history, even though you're using a VPN.



How a DNS leak occurs (source: www.darknessgate.com)

- ✔ To ensure that your VPN provider is not vulnerable to this risk, you are strongly advised to test your connection directly after connecting to your VPN provider, as follows:-
  - ✔ 1. Go to https://www.dnsleaktest.com.
  - ✔ 2. You will see two buttons along with your current IP address. The first button is labeled “Standard test,” and the second is “Extended test.” Click the second button for detailed results.
  - ✔ 3. The detailed results page will show you a list of all the DNS servers (along with their locations) that are used to resolve your typed website URLs into IP addresses. If any of these servers are not related to your VPN provider company, this means your connection is leaking information about you.
  - ✔ Reputable VPN providers have a connection leak prevention mechanism. However, you need to make sure that your VPN provider has this feature enabled automatically for your connection.
  - ✔ Do DNS leak testing, as explained, to assure that your DNS traffic is tunneled through your VPN-encrypted tunnel and not through your ISP.