

راهنمای تنظیمات حفاظتی مرورگرهای

فایرفاکس (Firefox) 

و

مایکروسافت اج (Microsoft Edge) 



دانشگاه سیستان و بلوچستان

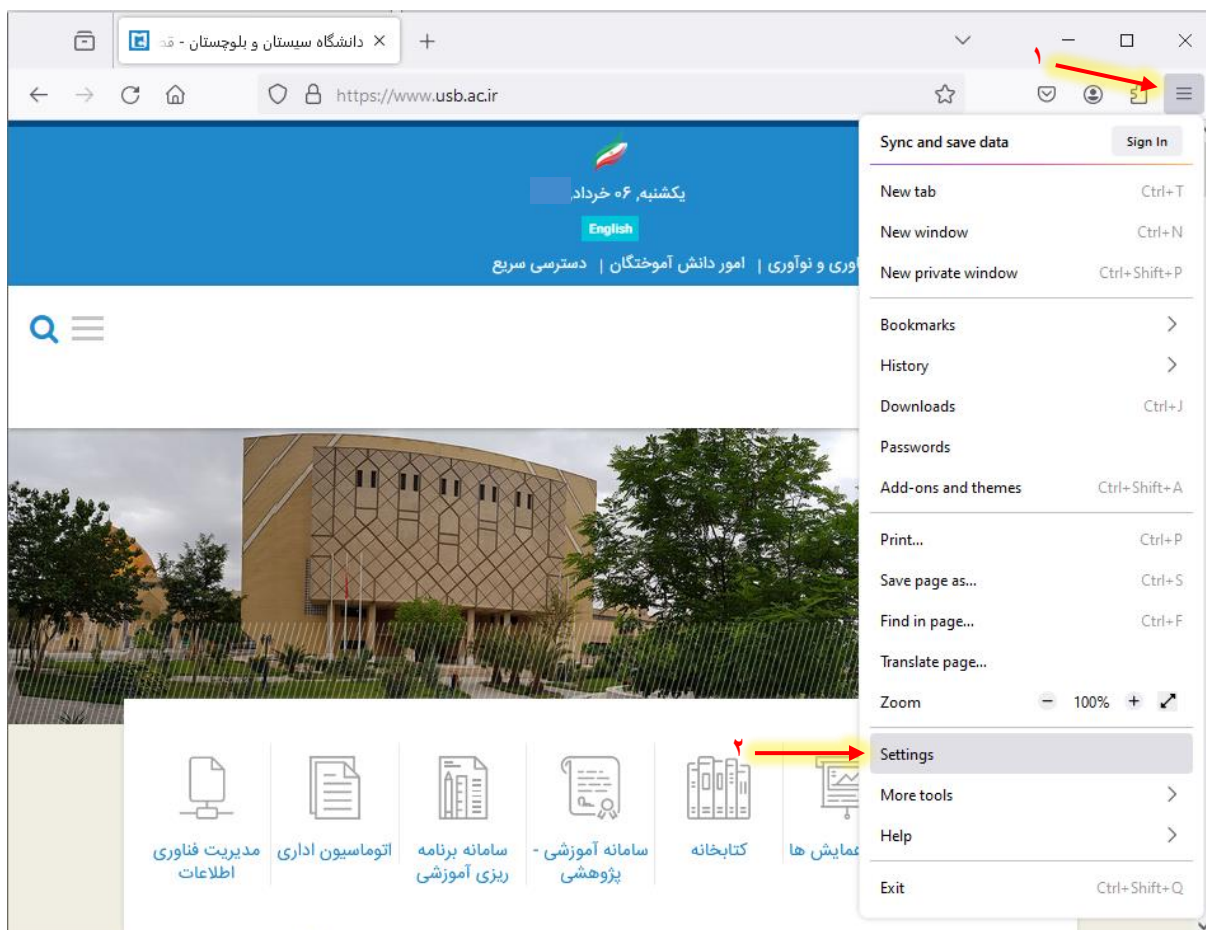


۱. بالا بردن امنیت حریم شخصی در مرورگرها

در این راهنما اقداماتی که می توان در دو مرورگر فایرفاکس (Firefox) و مایکروسافت اج (Microsoft Edge) جهت بالا بردن امنیت و حفظ حریم شخصی انجام داد، شرح داده می شود.

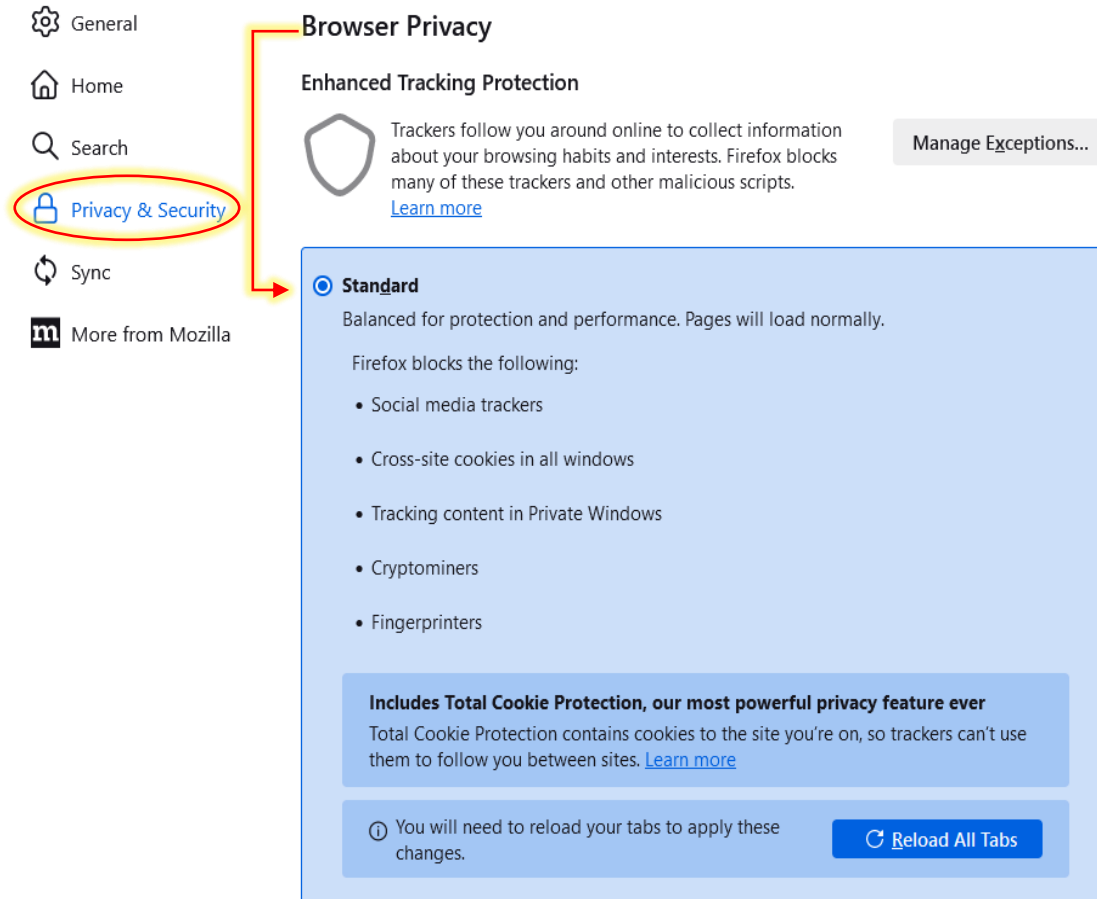
۱.۱. تنظیمات حفاظتی در مرورگر فایرفاکس

ابتدا مرورگر خود را باز کنید. سپس، با کلیک روی علامت سه خط در سمت راست بالای صفحه که در شکل (۱) نشان داده شده است، وارد قسمت تنظیمات (Setting) شوید و موارد ذیل را اعمال نمایید. تنظیمات انجام شده روی مرورگر اعمال شده و نیاز به ذخیره کردن ندارد.



شکل ۱. نحوه ورود به بخش تنظیمات مرورگر فایرفاکس

۱،۱،۱. تنظیم گزینه ی Enhanced Tracking Protection

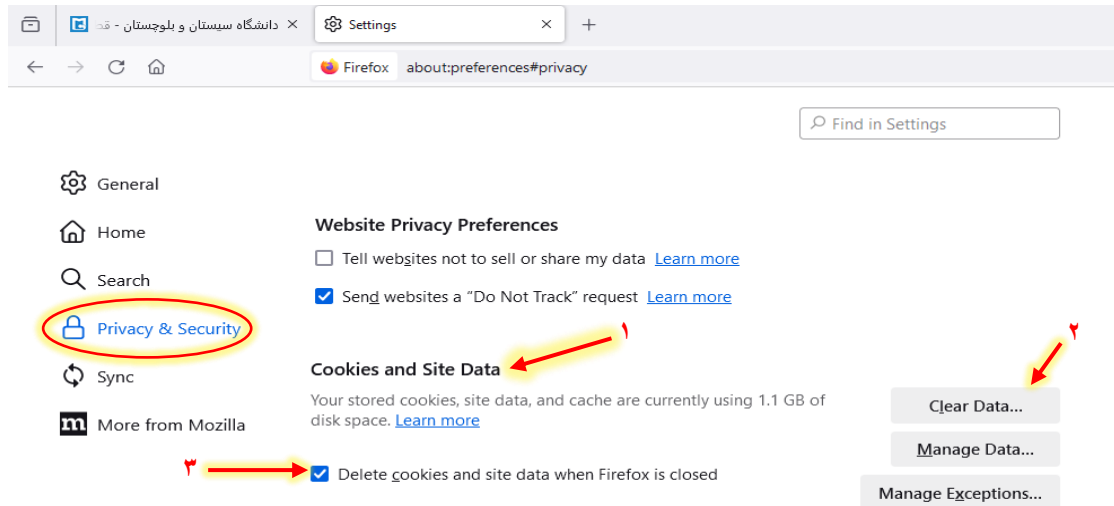


The screenshot shows the Firefox settings interface. On the left, a sidebar contains options: General, Home, Search, Privacy & Security (highlighted with a red circle), Sync, and More from Mozilla. The main content area is titled 'Browser Privacy' and features 'Enhanced Tracking Protection'. A shield icon is shown next to the text: 'Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.' A 'Manage Exceptions...' button is visible. Below this, the 'Standard' protection level is selected, described as 'Balanced for protection and performance. Pages will load normally.' A list of blocked items includes: Social media trackers, Cross-site cookies in all windows, Tracking content in Private Windows, Cryptominers, and Fingerprinters. A blue box highlights 'Includes Total Cookie Protection, our most powerful privacy feature ever' with a sub-note: 'Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. [Learn more](#)'. At the bottom, a message states 'You will need to reload your tabs to apply these changes.' and a 'Reload All Tabs' button is present.

شکل ۲. نحوه تغییر تنظیم Enhanced Tracking Protection

مطابق شکل (۲) وارد قسمت Privacy & Security شده و از بخش Browser Privacy تنظیم مربوط به Enhanced Tracking Protection را در حالت Standard قرار دهید.

۱،۱،۲. تنظیم کوکی ها (Cookies)



شکل ۳. نحوه تغییر تنظیم کوکی ها

مطابق شکل (۳) در همان قسمت قبل (Privacy) صفحه را کمی پایین تر برده و از بخش Cookies and Site Data تنظیمات مربوط به این بخش را طی مراحل ذیل انجام دهید:

- ✓ ابتدا روی گزینه ی Clear Data کلیک کرده تا اطلاعات ذخیره شده در کوکی ها، کش ها و حافظه مرورگر شما پاک شوند.
- ✓ سپس تیک گزینه ی Delete cookies and site data when Firefox is closed را بزنید تا بعد از هر بار استفاده از مرورگر، در زمان بسته شدن به صورت خودکار حافظه ی کش و کوکی ها پاک شوند.



۱,۱,۳. تنظیم Firefox Data Collection and Use

Find in Settings

- General
 - Block pop-up windows [Exceptions...](#)
 - Warn you when websites try to install add-ons [Exceptions...](#)
- Home
- Search
- Privacy & Security**
 - Firefox Data Collection and Use**

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information. [Privacy Notice](#)

ⓘ You're no longer allowing Mozilla to capture technical and interaction data. All past data will be deleted within 30 days. [Learn more](#)

 - Allow Firefox to send technical and interaction data to Mozilla [Learn more](#)
 - Allow Firefox to make personalized extension recommendations [Learn more](#)
 - Allow Firefox to install and run studies [View Firefox studies](#)
 - Allow Firefox to send backlogged crash reports on your behalf [Learn more](#)
- Sync
- More from Mozilla

غیرفعال سازی همه
گزینه های این قسمت

شکل ۴. نحوه تنظیم گزینه های Firefox Data Collection and Use

مطابق شکل (۴) با غیر فعال کردن کلیه تنظیمات این بخش می‌توانید مشخص کنید که موزیلا، اجازه ندارد که به اطلاعات عملکرد مرورگر شما دسترسی داشته باشد.



Deceptive Content and Dangerous Software Protection تنظیم ۱.۱.۴

HTTPS-Only Mode in all windows تنظیم ۱.۱.۵

The screenshot shows the Firefox Settings page for Security. The following options are checked:

- Deceptive Content and Dangerous Software Protection** (highlighted with a red box)
 - Block dangerous and deceptive content [Learn more](#)
 - Block dangerous downloads
 - Warn you about unwanted and uncommon software
- HTTPS-Only Mode** (highlighted with a red box)
 - Enable HTTPS-Only Mode in all windows
 - Enable HTTPS-Only Mode in private windows only
 - Don't enable HTTPS-Only Mode

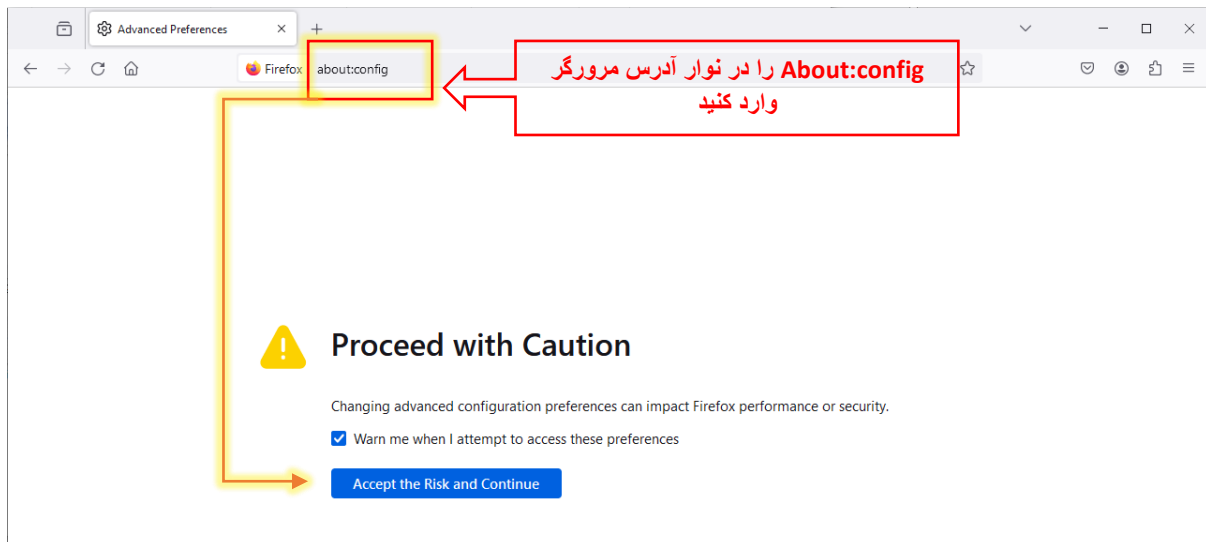
A red bracket groups the three checked options under the heading "فعال شدن همه گزینه ها".

شکل ۵. نحوه تنظیمات Security

مطابق شکل (۵) ابتدا تیک تمام گزینه های زیر مجموعه “Deceptive Content and Dangerous Software Protection” را بردارید. این کار Firefox را از به اشتراک گذاشتن اطلاعات مربوط به بازدیدهای شما از سایت های احتمالاً مخرب، باز می دارد. سپس در قسمت HTTPS-Only Mode گزینه اول Enable HTTPS-Only Mode in all windows را انتخاب کنید تا مرورگر، وب سایت ها را فقط در حالت ایمن باز نماید.

۱,۲. about:config

این تنظیمات یک راه برای بررسی و تغییر اولویت ها و تنظیمات فایرفاکس را فراهم می کند. این دستور برای ویرایش تنظیمات زیرساختی فایرفاکس کاربرد دارد. پس از وارد کردن آن ابتدا اخطاری به شما داده می شود که بیان گر میزان حساس بودن تنظیمات این بخش است.

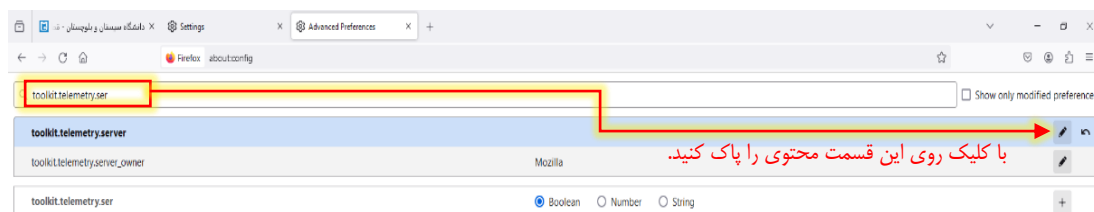


شکل ۶ نحوه باز کردن صفحه تنظیمات about:config

بعد از تایید این هشدار وارد صفحه تنظیمات اصلی می شوید.

حال در صفحه اصلی در نوار جستجو، هر یک از تنظیمات زیر را تایپ کنید و سپس آنها را روی مقدار ارائه شده در سمت راست تنظیم نمایید:

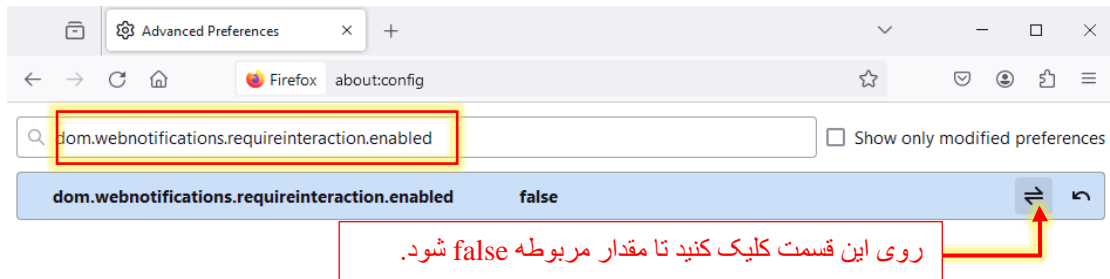
۱,۲,۱. تنظیمات toolkit.telemetry.server



شکل ۷. تنظیم toolkit

مطابق شکل (۷) عبارت toolkit.telemetry.server را در نوار جستجو وارد کرده و کلید Enter را بر روی کیبورد فشار دهید، سپس از طریق گزینه ی ویرایش سمت راست، محتوی را پاک کنید.

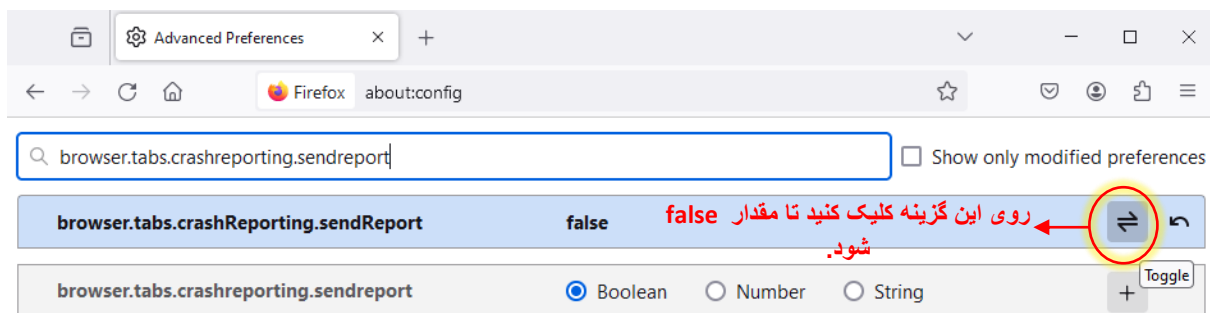
۱,۲,۲. تنظیمات webnotifications



شکل ۸. تنظیمات اعلان ها

مطابق شکل (۸) عبارت `dom.webnotifications.requireinteraction.enabled` را در نوار جستجو وارد کنید تا تنظیمات آن برای شما باز شود سپس از طریق گزینه ویرایش سمت راست عبارت، این گزینه را روی `False` تنظیم کنید تا Notification هر گونه وب سایت را به صورت کامل غیر فعال نماید.

۱,۲,۳. تنظیمات crashreporting



شکل ۹. تنظیمات crashreporting

مطابق شکل (۹) عبارت `browser.tabs.crashreporting.sendreport` را در نوار جستجو وارد کنید و مقدار آن را به `False` تغییر دهید.

۱,۲,۴. تنظیم دسترسی به موقعیت مکانی

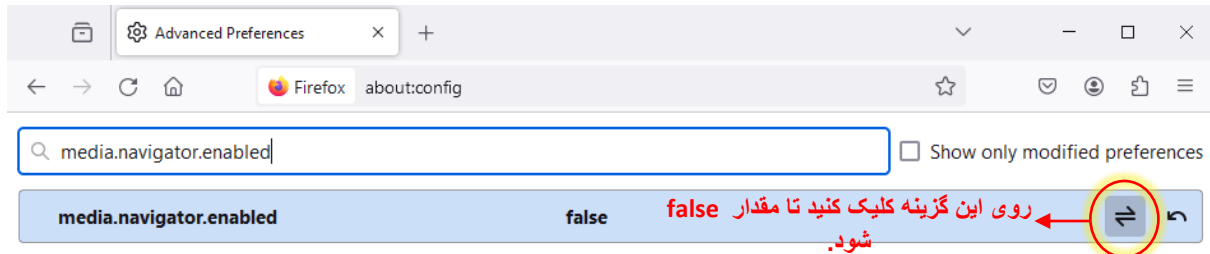


شکل ۱۰. نحوه تنظیم دسترسی موقعیت مکانی

مطابق شکل (۱۰) عبارت `geo.enabled` را در نوار جستجو وارد کرده و از طریق گزینه ی ویرایش مقدار را روی `False` تنظیم کنید تا مرورگر اجازه دسترسی به موقعیت مکانی شما نداشته باشد.



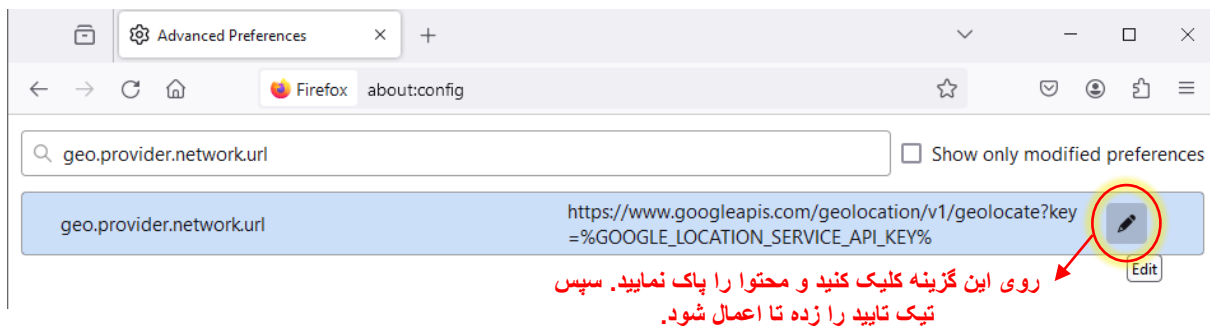
۱،۲،۵. تنظیمات دسترسی به دوربین و میکروفون



شکل ۱۱. نحوه تنظیم دسترسی به دوربین و میکروفون

مطابق شکل (۱۱) عبارت `media.navigator.enabled` را در نوار جستجو وارد کرده و مقدار آن را به `False` تغییر دهید. بدین صورت وب سایت ها مجوز دسترسی به میکروفون و دوربین را ندارند.

۱،۲،۶. تنظیمات حفاظت ردیابی



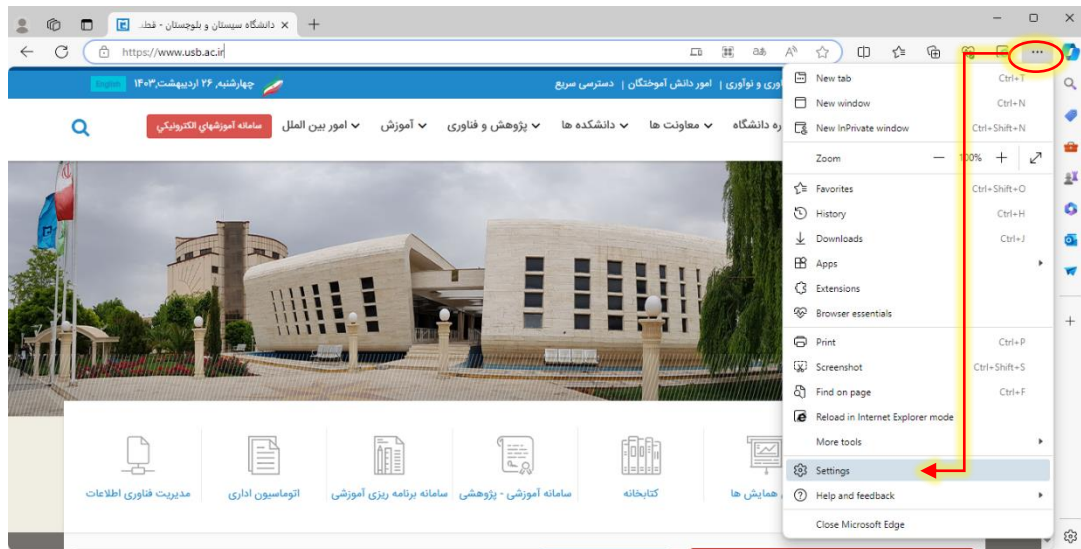
شکل ۱۲. نحوه تنظیم دسترسی به موقعیت مکانی `url`

مطابق شکل (۱۲) عبارت `geo.provider.network.url` را در نوار جستجو وارد کرده و با کلیک روی گزینه ویرایش، محتوای مربوطه را پاک کنید. اکنون وب سایت ها قادر به ردیابی کلیک های شما در هنگام استفاده از مرورگر نخواهند بود.



۲،۲. تنظیمات حفاظتی در مرورگر مایکروسافت اج

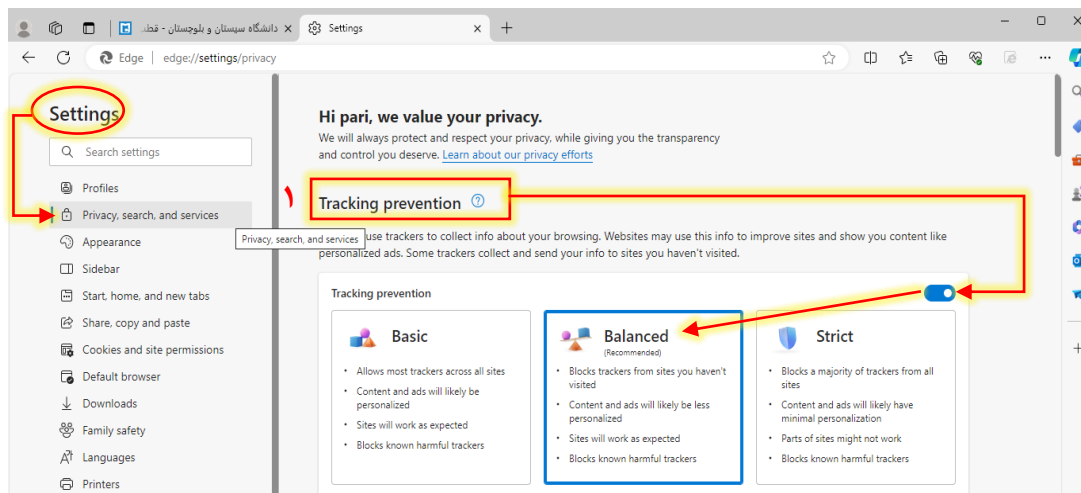
مرورگر خود را باز نموده و از قسمت ... در بالا سمت راست مرورگر، گزینه تنظیمات (Setting) را انتخاب نمایید تا وارد محیط تنظیمات شوید. (مطابق شکل ۲.۱)



شکل ۲.۱. نحوه ورود به صفحه تنظیمات مرورگر اج

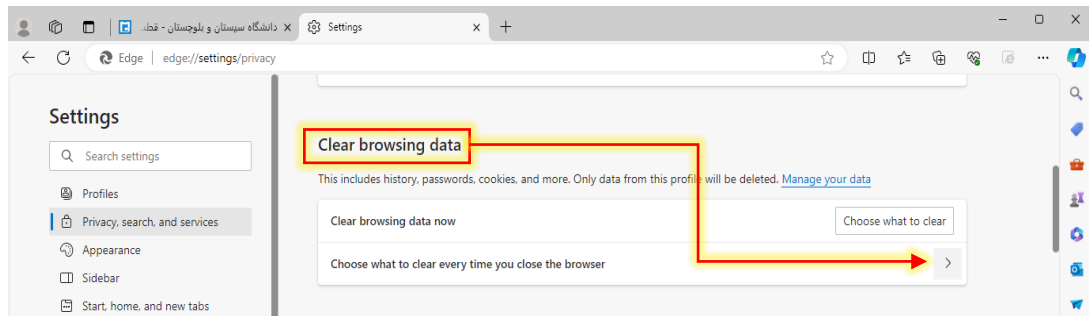
مطابق شکل (۲.۲) بعد از باز شدن صفحه تنظیمات وارد قسمت Privacy, search, and services شده و تنظیمات را به ترتیب و طبق تصاویر زیر انجام دهید.

۱. ابتدا گزینه Tracking prevention را فعال کرده و در حالت Balanced قرار دهید:



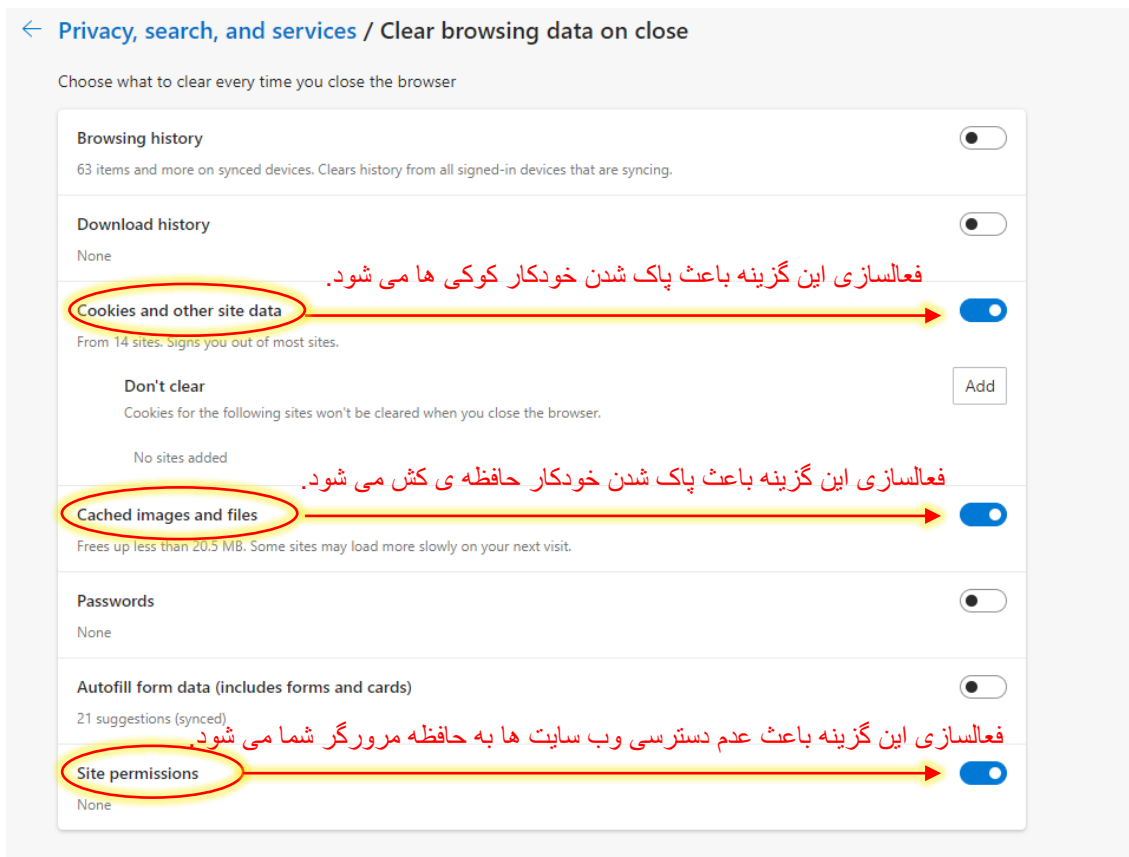
شکل ۲.۲. نحوه تنظیم حالت tracking

۲. در همان صفحه کمی پایین تر رفته و در قسمت Clear browsing data روی فلش مشخص شده کلیک کرده و طبق تصویر گزینه های مشخص شده را فعال نمایید:



شکل ۲.۳. تنظیم کوکی ها و حافظه

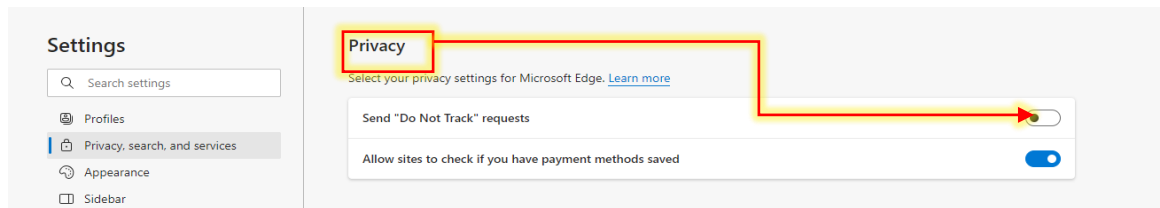
✓ بعد از کلیک روی علامت فلش وارد صفحه زیر شده و گزینه های مشخص شده در شکل زیر را فعال نمایید، سپس جهت ادامه تنظیمات از قسمت بالای صفحه روی فلش برگشت کلیک کنید.



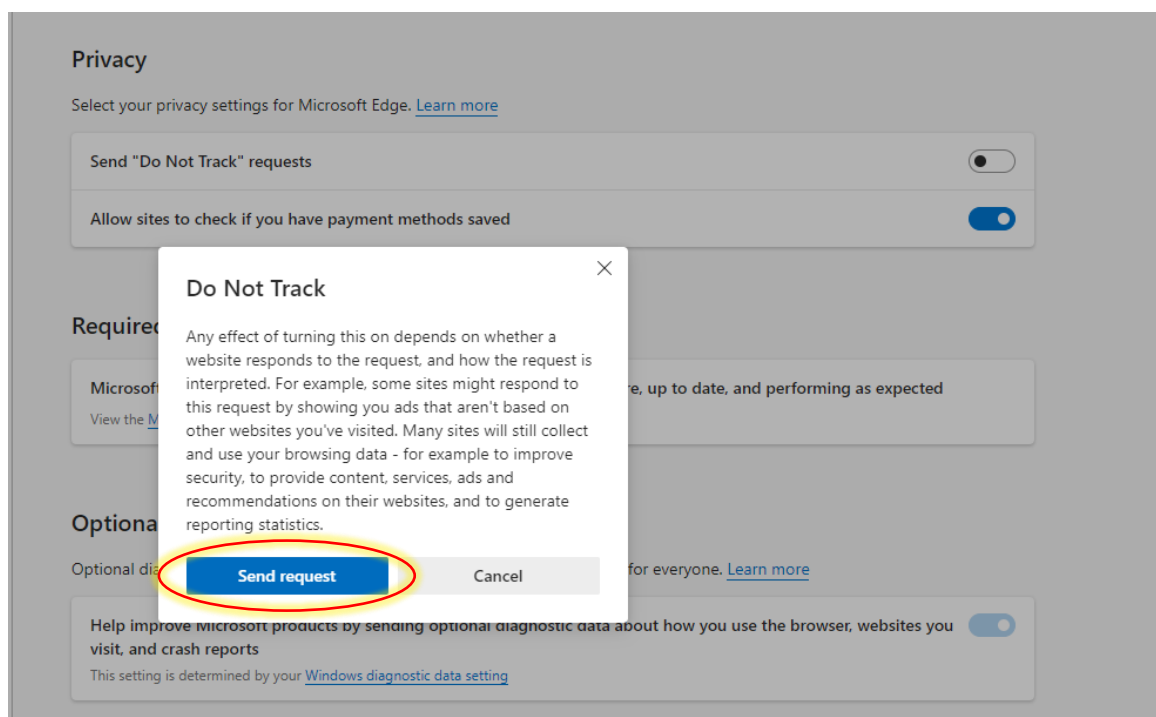
شکل ۲.۴. نحوه فعالسازی پاک کردن خودکار کوکی ها و کش در مرورگر

مطابق شکل (۲.۴) سه مورد مشخص شده را فعال کنید سپس با کلیک روی علامت برگشت بالای صفحه به تنظیمات اصلی برگردید.

۳. قسمت بعدی **Privacy** است که با کمی پایین تر آمدن در همان صفحه اصلی آن را مشاهده می کنید. در این قسمت گزینه ی **send “Do Not Track” requests** را فعال کنید(مطابق شکل ۲.۵).



شکل ۲.۵. نحوه ورود به تنظیم Privacy



شکل ۲.۶. تنظیم حالت Do Not Track

مطابق شکل (۲.۶) در پنجره ی باز شده بایستی جهت ادامه گزینه **Send request** را انتخاب نمایید.