راهنمای تنظیمات حفاظتی مرورگرهای

فایرفاکس (Firefox)

و

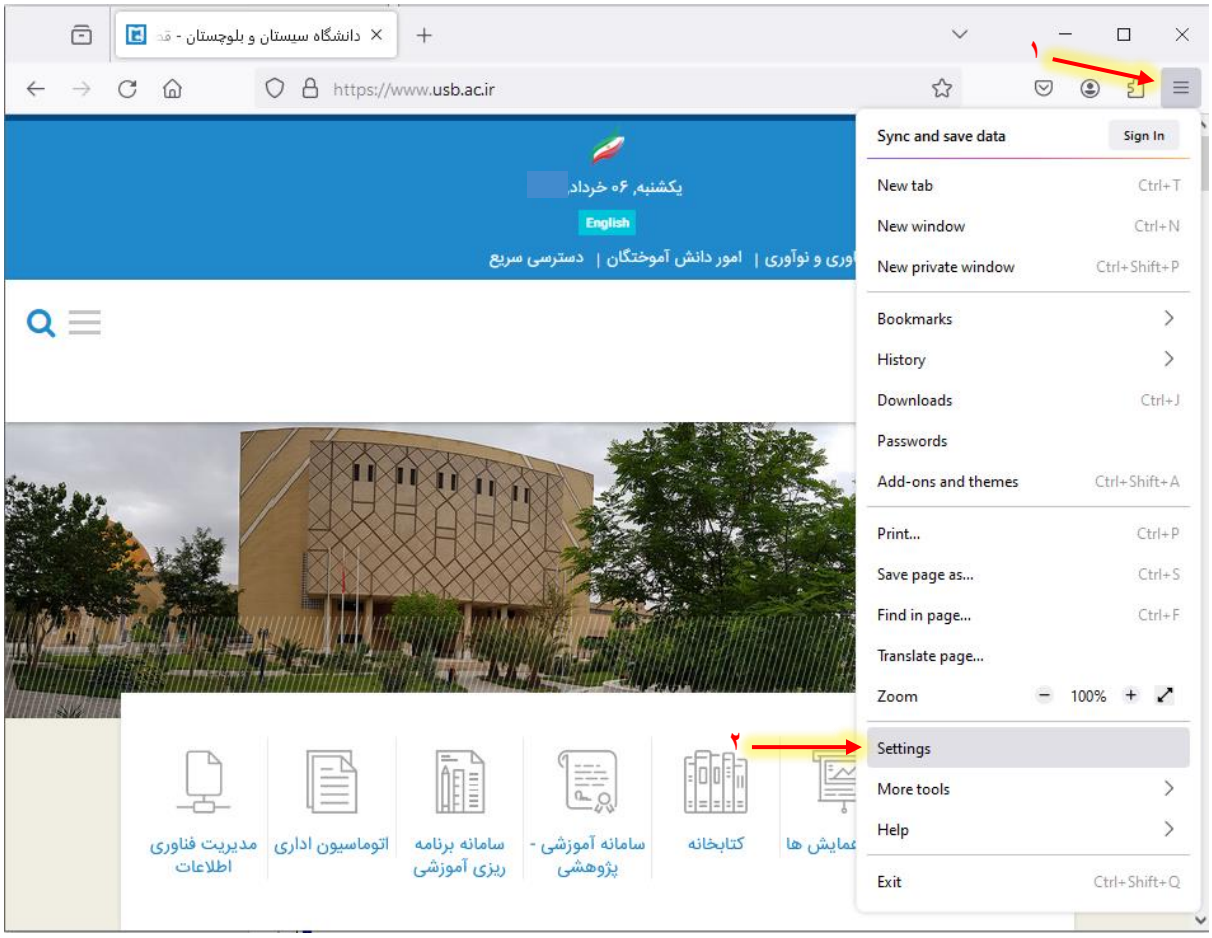
مایکروسافت اج (Microsoft Edge)

۱. بالا بردن امنیت حریم شخصی در مرورگر ها

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

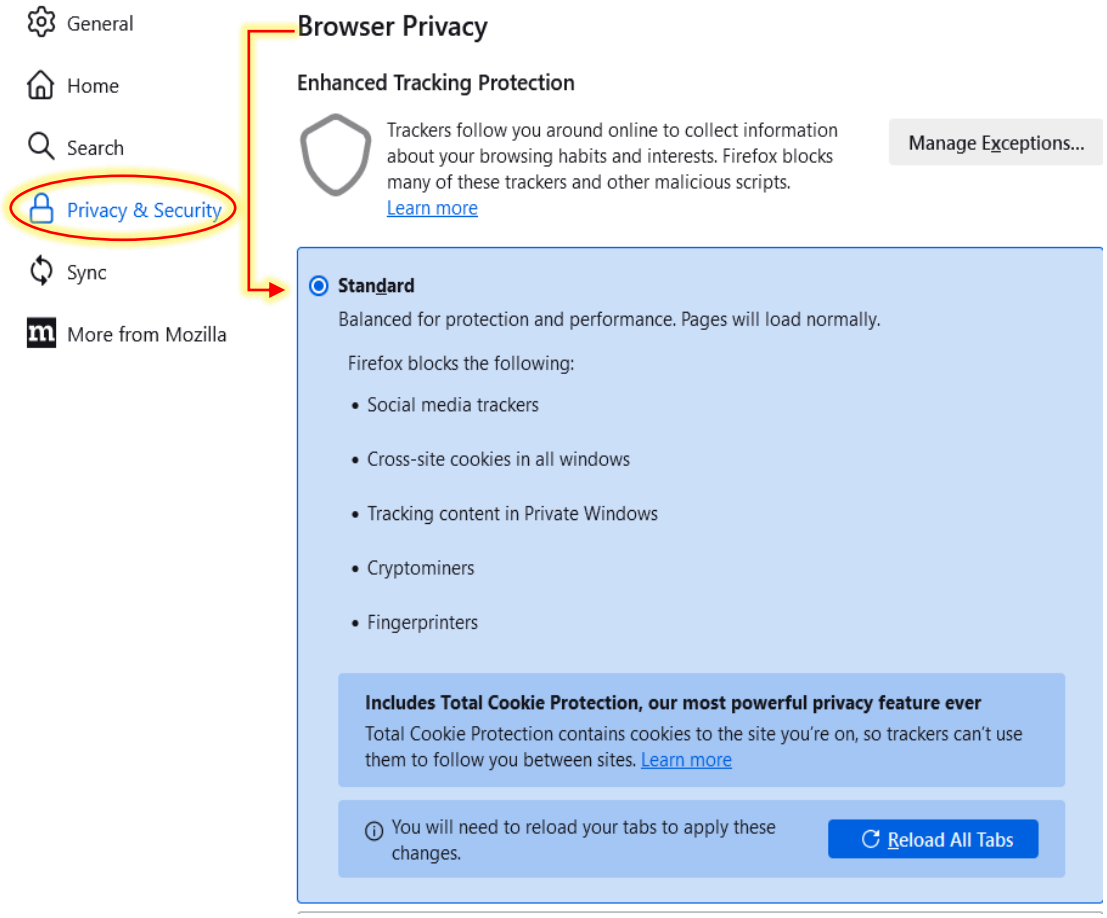
۱,۱. تنظیمات حفاظتی در مرورگر فایرفاکس

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

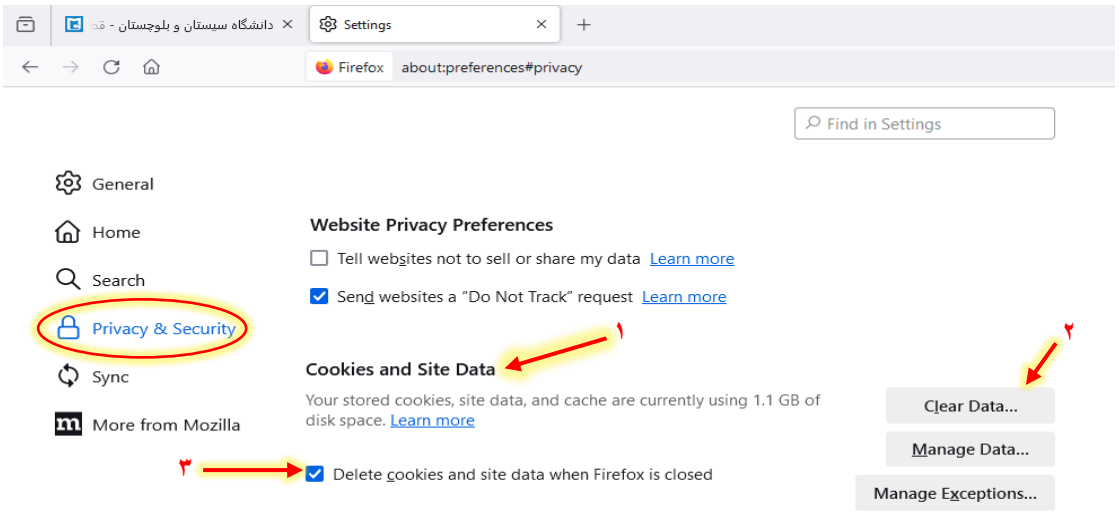
۱،۱،۱. تنظیم گزینه ی Enhanced Tracking Protection



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 کوکی‌ها (Cookies)

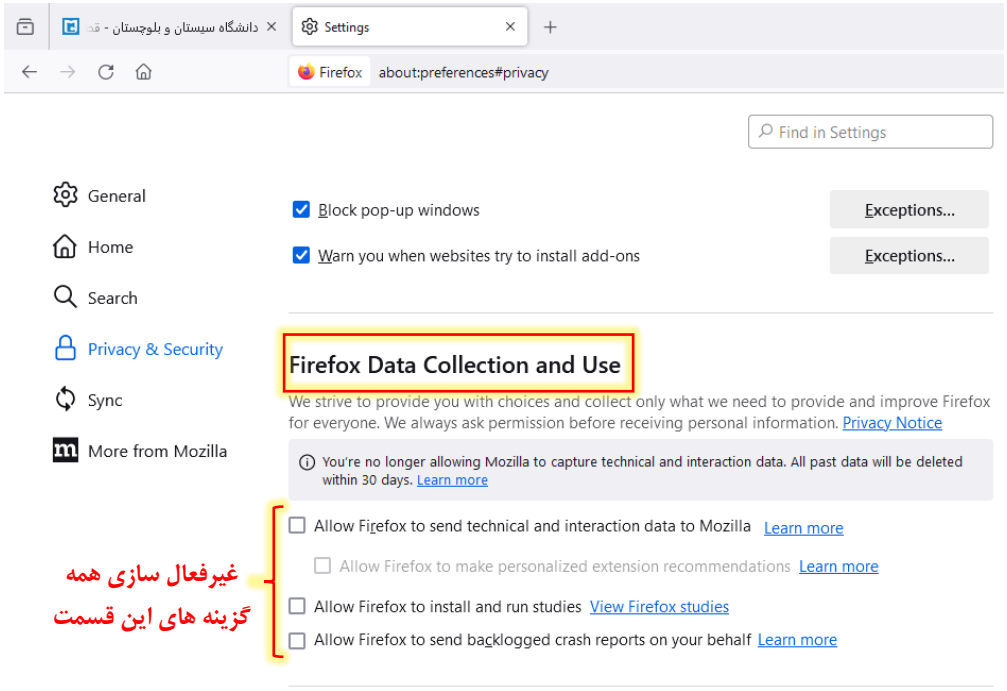


شکل ۳. نحوه تغییر تنظیم کوکی ها

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 مروگر، در زمان بسته شدن به صورت خودکار حافظه ی کش و کوکی ها پاک شوند.

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

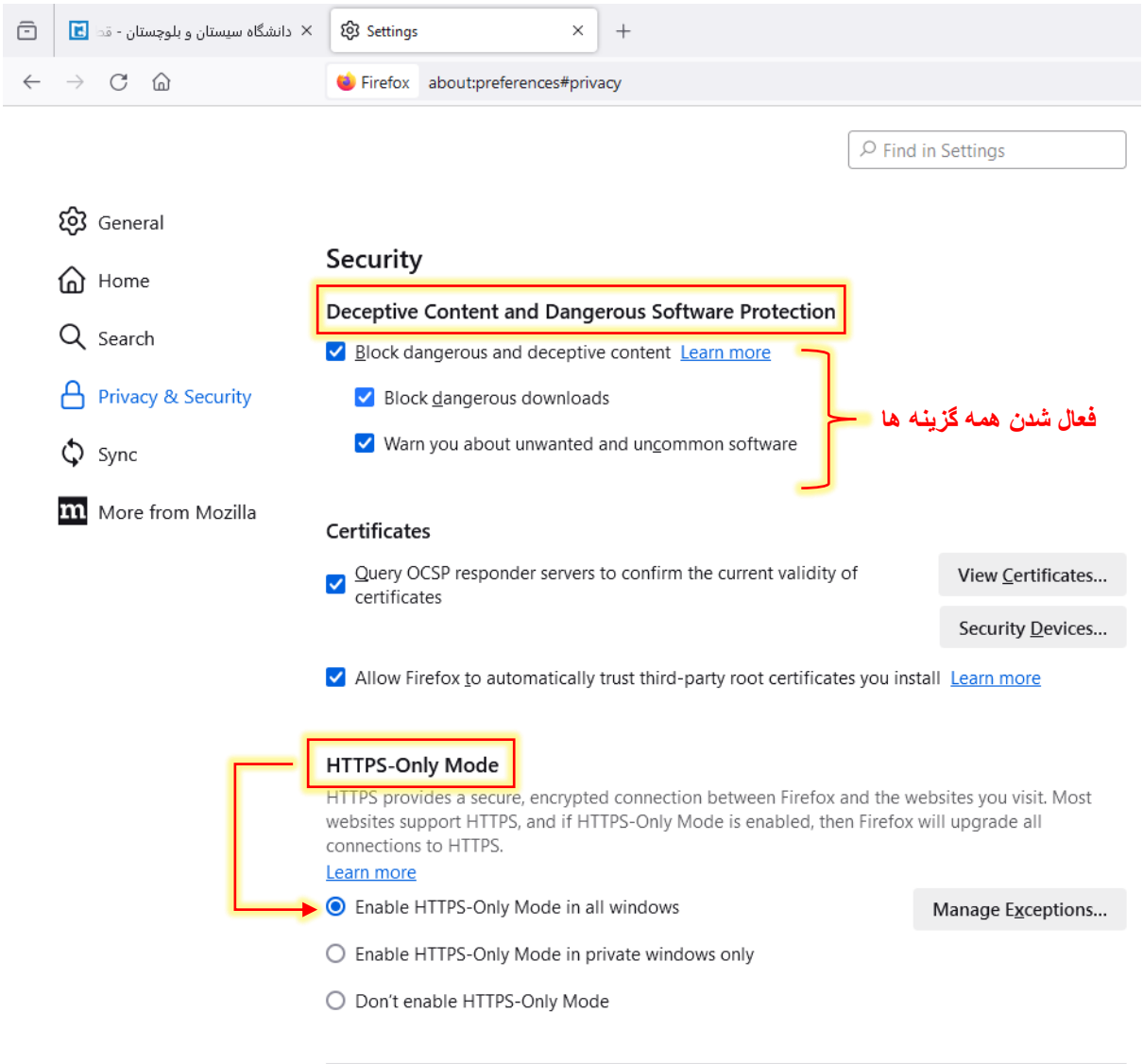


شکل ۴. نحوه تنظیم گزینه های Firefox Data Collection and Use

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 .

۱،۱،٤. تنظیم Deceptive Content and Dangerous Software Protection

۱،۱،٥. تنظیم HTTPS-Only Mode in all windows

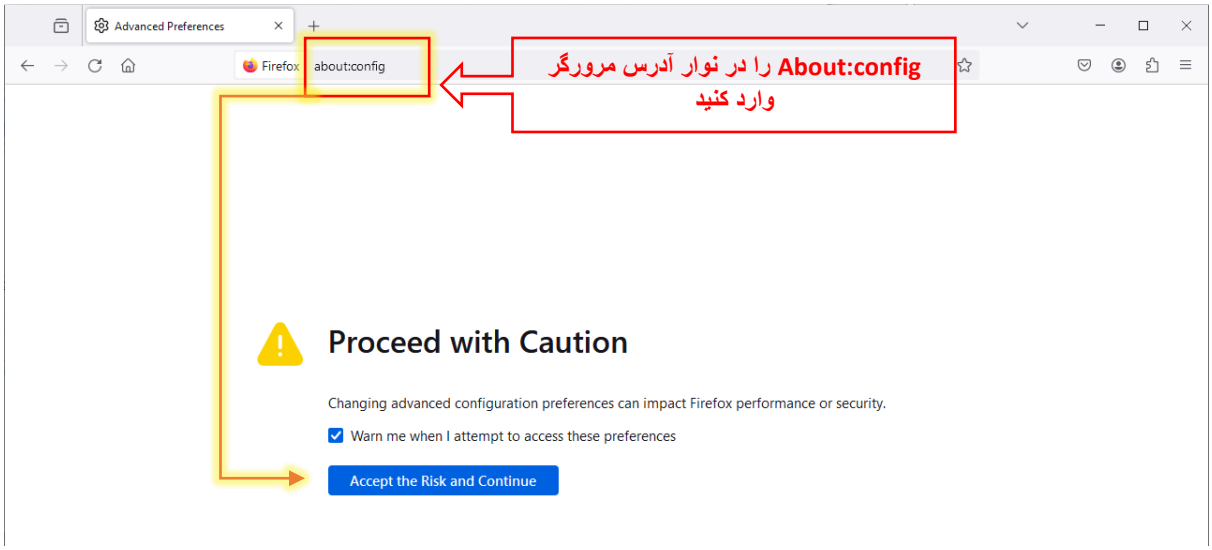


شکل ۵. نحوه تنظیمات Security

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 می‌شود که بیان‌گر میزان حساس بودن تنظیمات این بخش است.

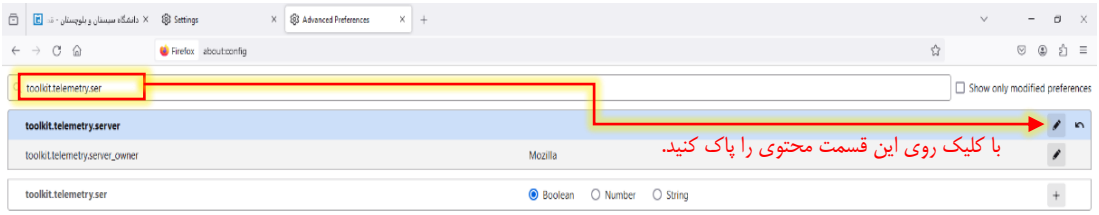


شکل ۶ نحوه باز کردن صفحه تنظیمات about:config

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:

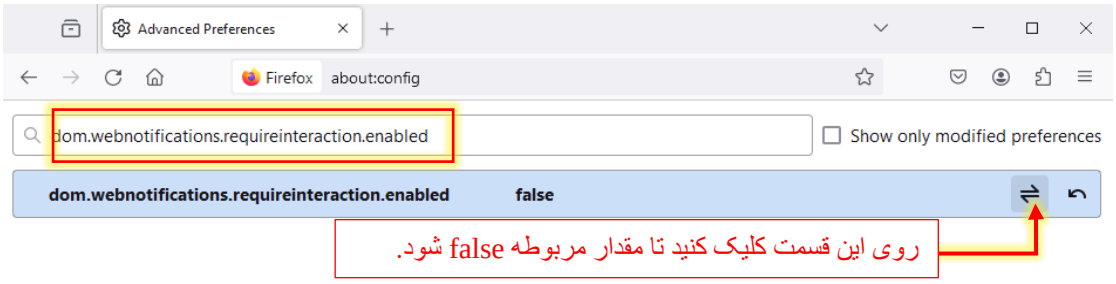
۱،۲،۱ **تنظیمات** toolkit.telemetry.server



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.

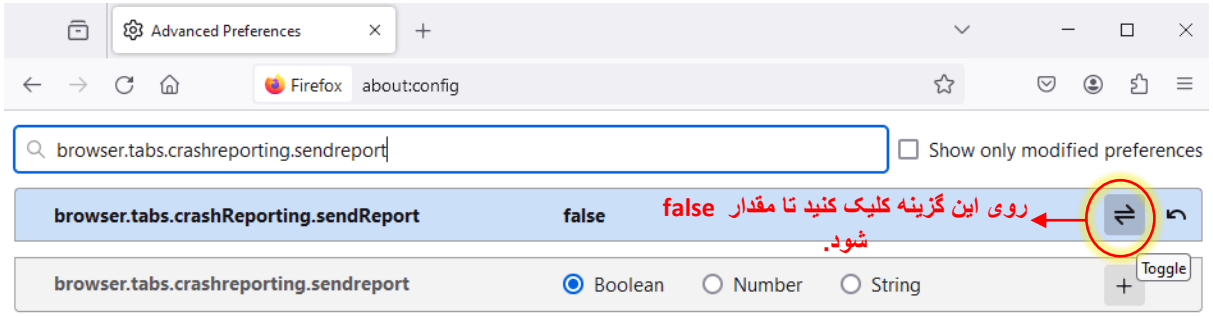
۱،۲،۲. تنظیمات webnotifications



شکل ۸ . تنظیمات اعلان ها

مطابق شـــکل (۸) عبارت dom.webnotifications.requireinteraction.enabled را در نوار جســـتجو 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 نمایید.

۱،۲،۳. تنظیمات crashreporting



شکل ۹ . تنظیمات crashreporting

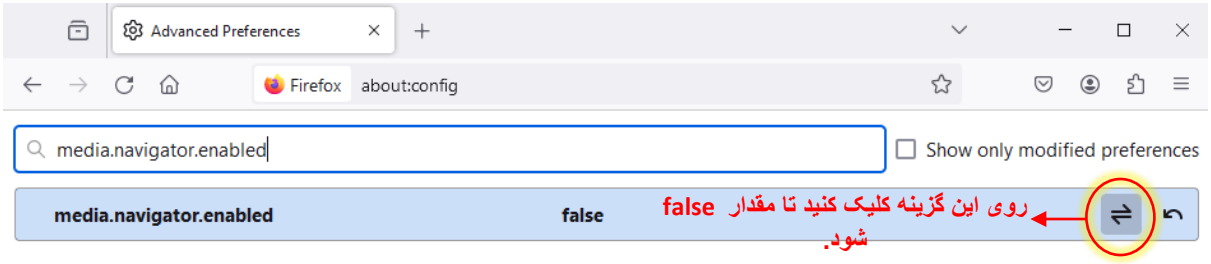
مطابق شکل (۹) عبارت browser.tabs.crashreporting.sendreport را در نوار جستجو وارد کنید و مقدار آن را به False تغییر دهید.

۱،۲،٤. 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.

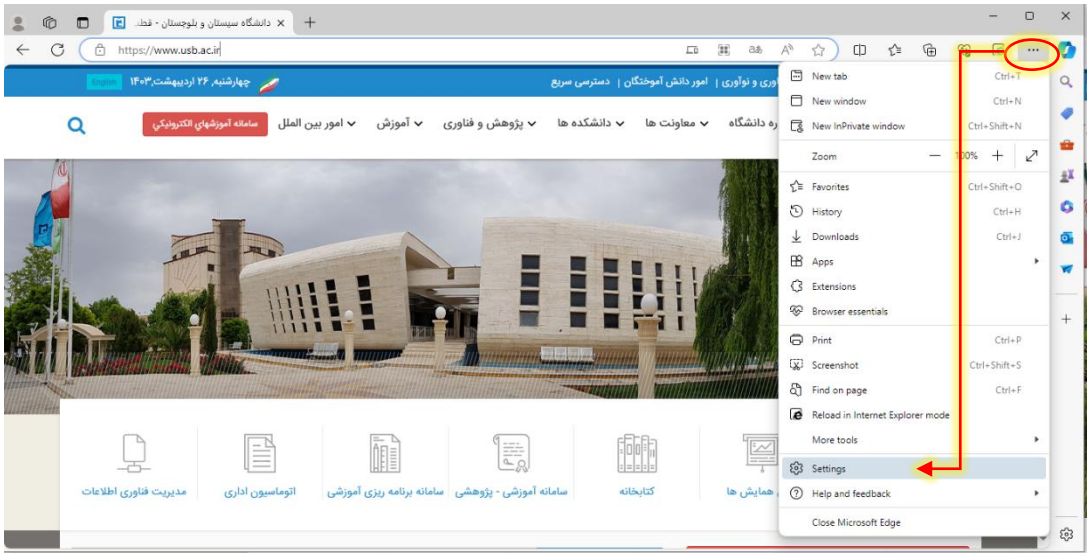
۱,۲,۶. تنظیمات حفاظت ردیابی

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 مروگر مایکروسافت اِج

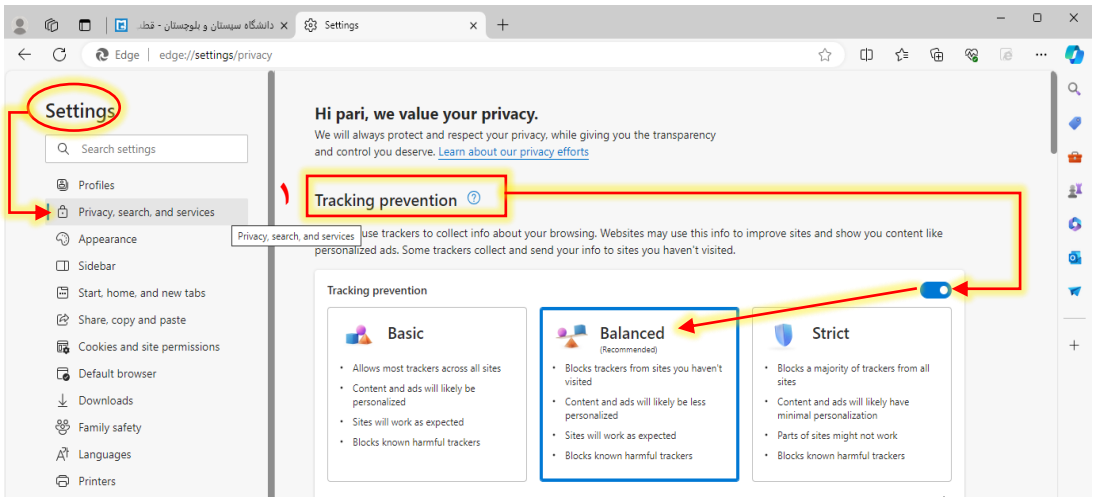
مرورگر خود را باز نموده و از قسمت ... در بالا سمت راست مرورگر، گزینه تنظیمات (Setting) را انتخاب نمایید تا وارد محیط تنظیمات شوید. (مطابق شکل ۲.۱)



شکل ۲.۱. نحوه ورود به صفحه تنظیمات مرورگر اج

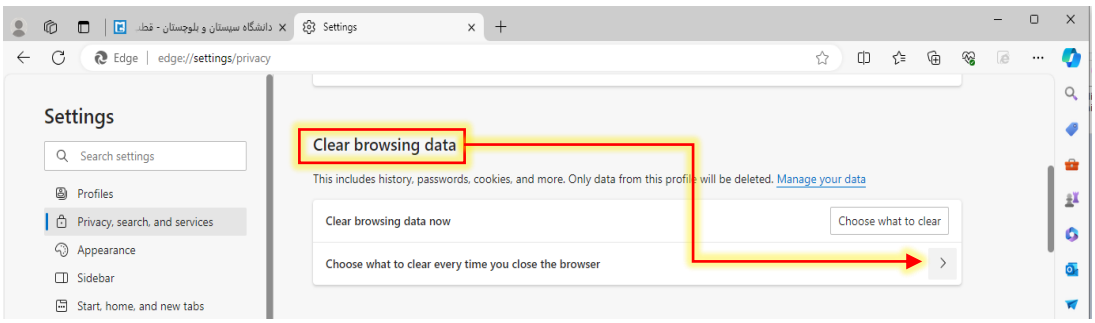
مطابق شکل(۲.۲) بعد از باز شدن صفحه تنظیمات وارد قسمت Privacy, search, and services شده و تنظیمات را به ترتیب و طبق تصاویر زیر انجام دهید.

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



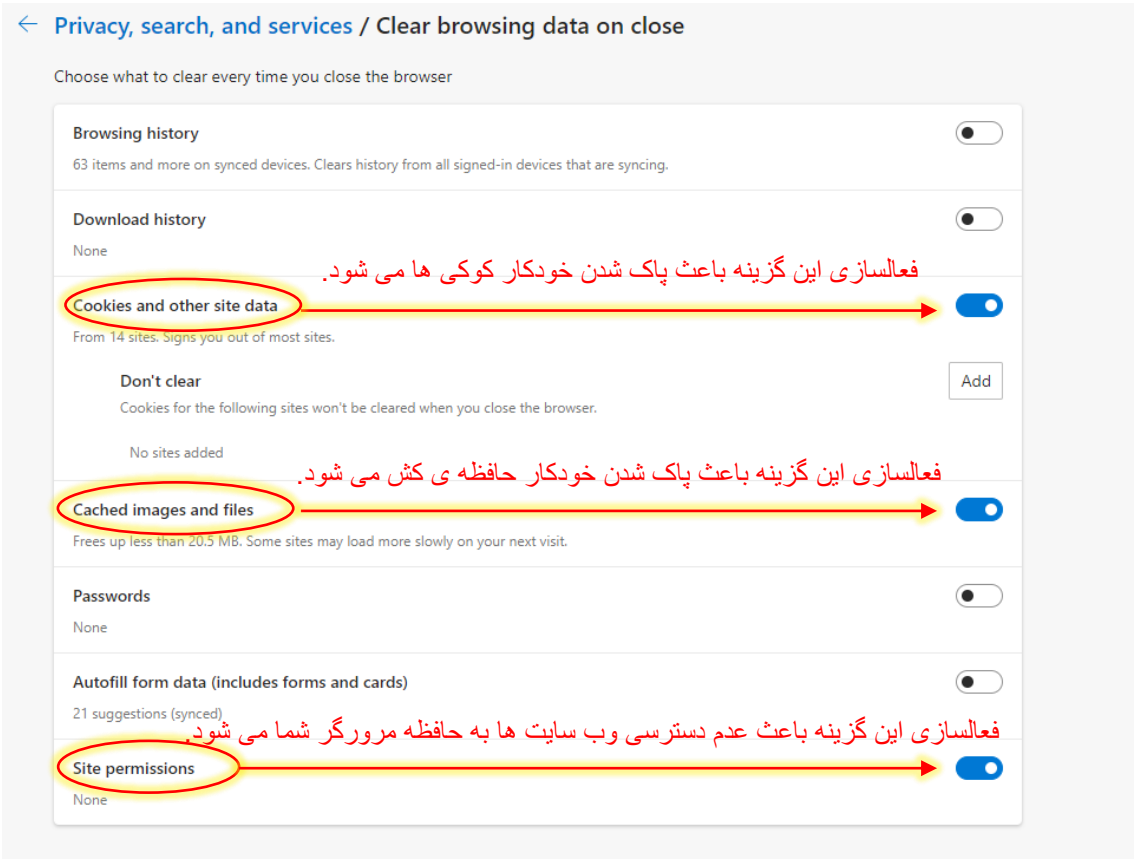
شکل ۲.۲. نحوه تنظیم حالت tracking

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

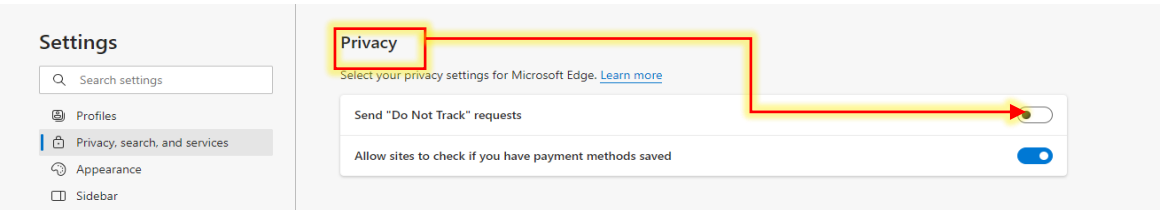
✓ بعد از کلیک روی علامت فلش وارد صفحه زیر شده و گزینه های مشخص شده در شکل زیر را فعال نمایید، سپس جهت ادامه تنظیمات از قسمت بالای صفحه روی فلش برگشت کلیک کنید.



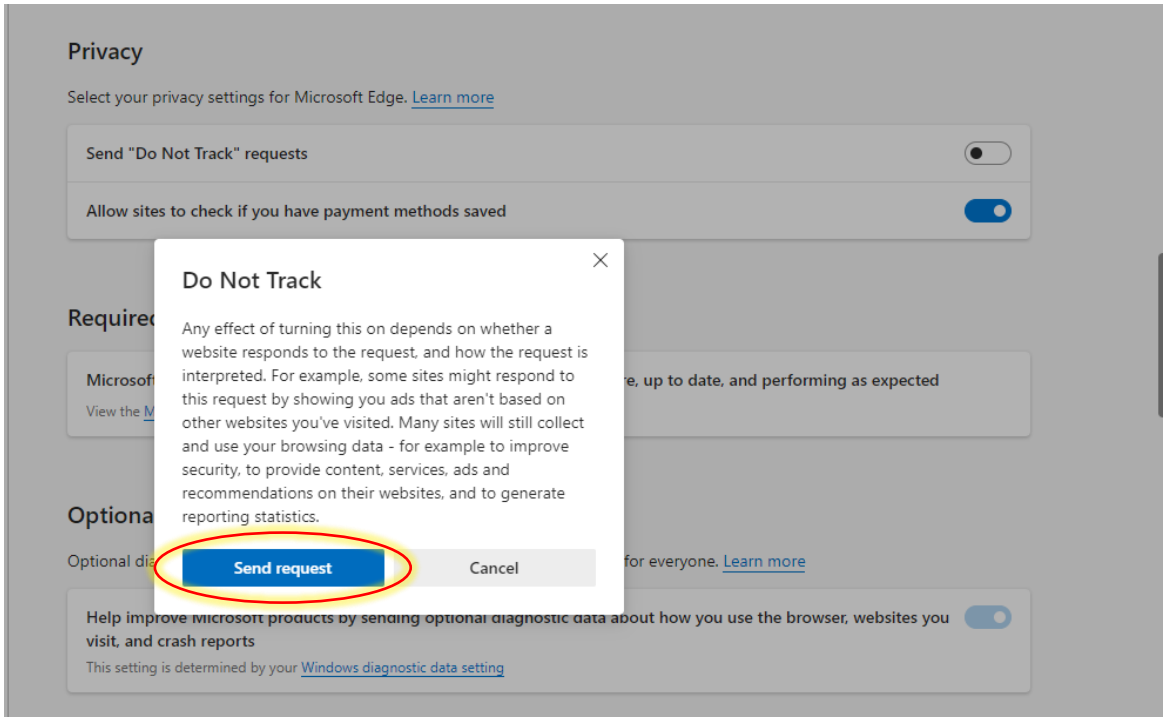
شکل ۲.۴. نحوه فعالسازی پاک کردن خودکار کوکی ها و کش در مرورگر

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.