



## چگونه مرورگر خود را ایمن کنیم؟

### ۱- ایمن سازی مرورگر Firefox

در این بخش به معرفی تنظیمات فایرفاکس به منظور ارتقا سطح امنیت و حفظ حریم خصوصی می‌پردازیم. این مراحل نیز در مرورگرهای دیگر قابل اجرا هستند.

#### ۱-۱- به روز رسانی

به منو ≡ در فایرفاکس مراجعه و با کلیک بر روی Help از انتهای منو، About Firefox را انتخاب کنید و از بروز بودن نسخه‌ی فایرفاکس اطمینان حاصل کنید.

همچنین به مسیر **Settings > General** مراجعه و در سربرگ Firefox Update گزینه ( Automatically install updates recommended ) را فعال کنید تا فایرفاکس همواره بروز نگه داشته شود.

#### ۱-۲- گواهینامه

بعضی از وبسایت‌ها از شما درخواست گواهینامه‌ی شخصی می‌کنند. برای اینکه مطمئن شوید که این پیام به صورت خودکار برای شما ارسال نشده‌است مسیر **Settings > Privacy & Security > Certificates** را دنبال و برای تنظیمات تیک دو گزینه‌ی زیر فعال باشد.



## چگونه مرورگر خود را ایمن کنیم؟

- General
- Home
- Search
- Privacy & Security**
- Sync
- More from Mozilla

### Security

#### Deceptive Content and Dangerous Software Protection

- Block dangerous and deceptive content [Learn more](#)
- Block dangerous downloads
- Warn you about unwanted and uncommon software

#### Certificates

- Query OCSP responder servers to confirm the current validity of certificates
- Allow Firefox to automatically trust third-party root certificates you install [Learn more](#)

[View Certificates...](#)

[Security Devices...](#)

### تصویر ۱- گواهینامه

#### ۳-۱- حفاظت از داده

در همان بخش **Settings > General** ، سربرگ **Network Settings** را انتخاب و بررسی کنید که هیچ کدام از چک باکس‌ها در حالت انتخاب شده نباشند. با این کار مطمئن می‌شوید که موزیلا هیچ گونه اطلاعاتی را در مورد سوابق جستجوهای شما ذخیره نکرده است.

#### ۴-۱- تنظیمات امنیتی

در مسیر **Settings > Privacy & Security > Security** ، چک باکس موارد نشان داده شده را انتخاب کنید . با فعال کردن این گزینه‌ها از هرگونه فیشینگ، دانلود خودکار و اجرای نرم افزارهای ناخواسته جلوگیری می‌شود.



## چگونه مرورگر خود را ایمن کنیم؟

- General
- Home
- Search
- Privacy & Security**
- Sync
- More from Mozilla

### Security

#### Deceptive Content and Dangerous Software Protection

- Block dangerous and deceptive content [Learn more](#)
- Block dangerous downloads
- Warn you about unwanted and uncommon software

### تصویر ۲- تنظیمات امنیتی

سپس طبق تصویر زیر بر روی **Manage Exceptions** روبه روی مورد **Warn you when sites try to install add-ons** کلیک کنید و تمام وبسایت‌هایی را که در این بخش اضافه نموده‌اید (حتی وبسایت‌های Mozilla Firefox) حذف کنید. با این کار برای نصب شدن هر اکستنشن بر روی مرورگر، نیاز به تاییدیه شماست.

- General
- Home
- Search
- Privacy & Security**
- Sync
- More from Mozilla

### Permissions

- Location [Settings...](#)
- Camera [Settings...](#)
- Microphone [Settings...](#)
- Speaker Selection [Settings...](#)
- Notifications [Learn more](#) [Settings...](#)
- Autoplay [Settings...](#)
- Virtual Reality [Settings...](#)
- Block pop-up windows [Exceptions...](#)
- Warn you when websites try to install add-ons [Exceptions...](#)

### تصویر ۳- تاییدیه



## چگونه مرورگر خود را ایمن کنیم؟

در ادامه‌ی همین صفحه نیز در بخش Passwords، بررسی کنید که چک باکس‌ها تیک نداشته باشند و هرچیزی را که در این قسمت ذخیره شده‌است حذف نمایید. با این کار پسوردهایی که قبلا در مرورگر شما برای وبسایت‌های مختلف ذخیره شده‌اند حذف می‌شوند. بنابراین قبلا اطمینان حاصل کنید که همه آن پسوردها را در جایی دیگر داشته باشید.

General

Home

Search

Privacy & Security

Sync

More from Mozilla

**Passwords**

Ask to save passwords [Exceptions...](#)

Fill usernames and passwords automatically

Suggest strong passwords

Suggest Firefox Relay email masks to protect your email address [Learn more](#)

Show alerts about passwords for breached websites [Learn more](#)

Use a Primary Password [Learn more](#) [Change Primary Password...](#)  
Formerly known as Master Password

Allow Windows single sign-on for Microsoft, work, and school accounts [Learn more](#)  
Manage accounts in your device settings

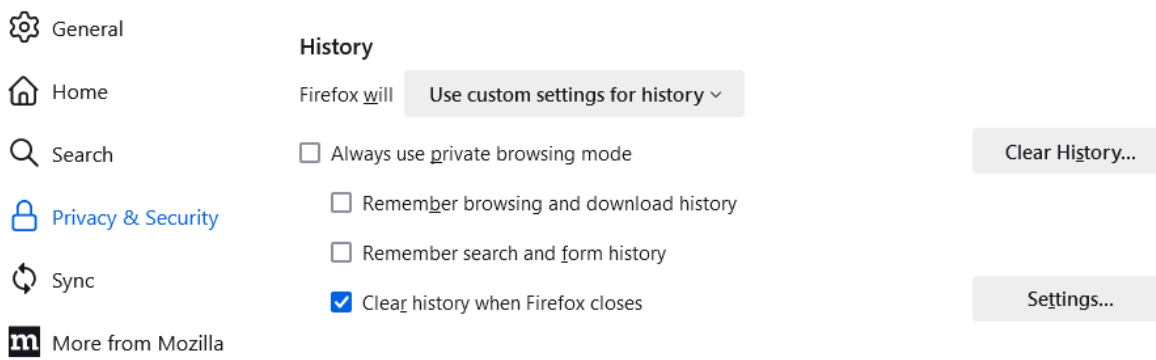
### تصویر ۴- پسورد

در تصویر زیر، تنظیمات بخش حریم خصوصی (Privacy) را مشاهده می‌کنید که با تنظیم کردن برخی موارد به صورت دستی می‌توانید بخش History مرورگر خود را مدیریت کنید. برای این کار باید در مسیر

### ≡ > Settings > Privacy & Security > History

از لیست روبه روی Firefox will مورد Use custom setting for history را انتخاب نمایید و در مواردی که پس از انتخاب این گزینه در اختیار شما قرار می‌گیرد، تیک گزینه‌ی Clear history when FireFox closes را بزنید. با این اقدام بعد از بستن فایرفاکس کلیه سوابق مرور صفحات وب از فایرفاکس حذف می‌شود. این اقدام مخصوصا برای سیستم‌هایی که در اختیار چند نفر به طور مشترک قرار می‌گیرند بسیار حائز اهمیت است.

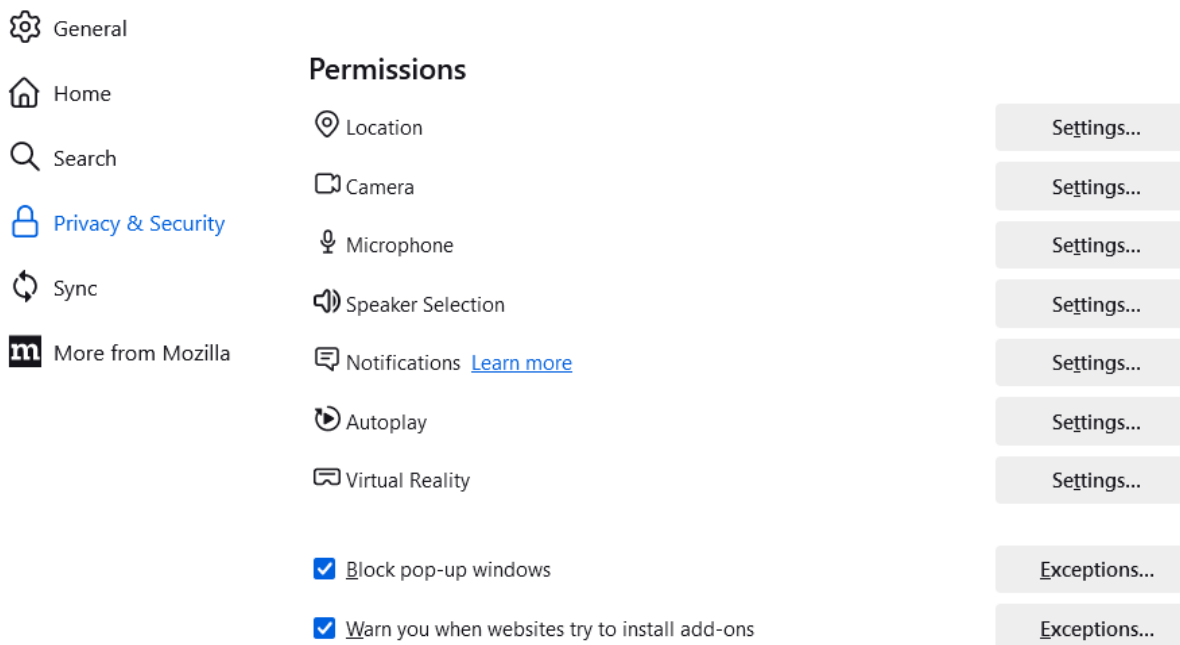
## چگونه مرورگر خود را ایمن کنیم؟



The screenshot shows the Firefox History settings page. On the left is a navigation menu with options: General, Home, Search, Privacy & Security (highlighted), Sync, and More from Mozilla. The main content area is titled 'History' and shows 'Firefox will Use custom settings for history'. Below this are several checkboxes: 'Always use private browsing mode', 'Remember browsing and download history', 'Remember search and form history', and 'Clear history when Firefox closes' (which is checked). On the right side, there are two buttons: 'Clear History...' and 'Settings...'.

### تصویر ۵- تاریخچه

مسیر **Settings > Privacy & Security > Permissions** را دنبال کنید و تیک گزینه **Block pop-up window** را بزنید و در بخش **Exception** روبه روی آن، تمام موارد ذخیره شده را حذف نمایید.



The screenshot shows the Firefox Permissions settings page. The left navigation menu is the same as in the previous image, with 'Privacy & Security' highlighted. The main content area is titled 'Permissions' and lists various permissions: Location, Camera, Microphone, Speaker Selection, Notifications (with a 'Learn more' link), Autoplay, and Virtual Reality. Each of these has a 'Settings...' button to its right. At the bottom, there are two checked checkboxes: 'Block pop-up windows' and 'Warn you when websites try to install add-ons'. To the right of these checkboxes are 'Exceptions...' buttons.

### تصویر ۶- دسترسی



## چگونه مرورگر خود را ایمن کنیم؟

### ۱-۵- افزونه ها و اکستنشن ها

در مسیر **Services > Add-ons and themes > ≡** هیچ برنامه‌ای را در حالت نصب شده نداشته باشید. احتمالاً در بخش **Add-ons > plugins** فایلی با عنوان **OpenH264 Video Codec provided by Cisco Systems** را می‌بینید که باید آن را به حالت **Never Activate** تنظیم نمایید. حتی ممکن است پلاگین‌های دیگری را داشته باشید که بهتر است آن‌ها را حذف و یا غیرفعال کنید. در حالت کلی برای هر پلاگین خود بهتر است گزینه‌ی **Ask to Activate** را انتخاب نمایید تا برای فعال شدن نیاز به تأیید شما باشد.

تعدادی از پلاگین‌های کاربردی فایرفاکس:

- [Disconnect](#) ❖
- [uBlock Origin](#) ❖
- [HTTPS Everywhere](#) ❖
- [NoScript](#) ❖
- [Self-Destructing Cookies](#) ❖



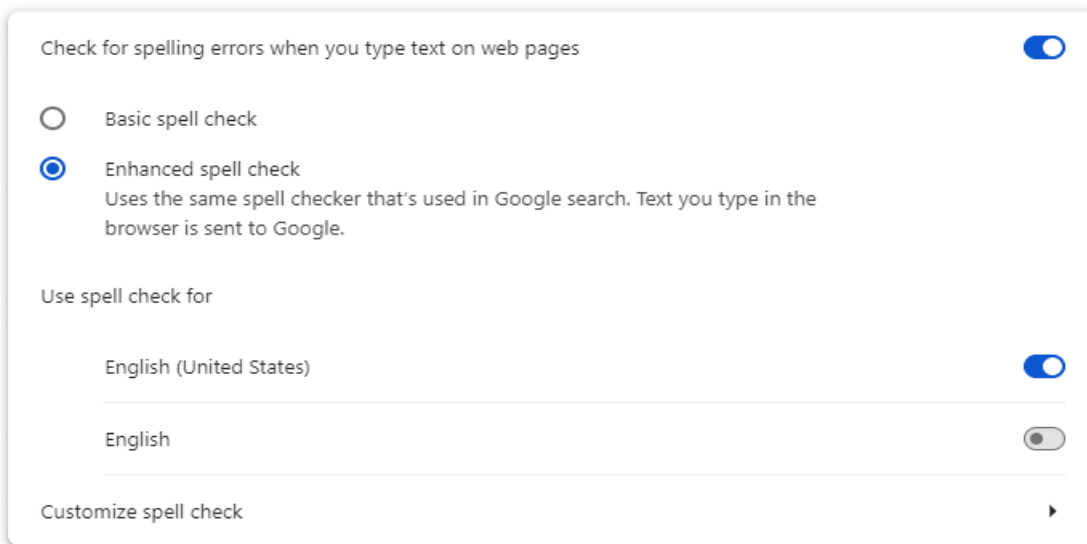
## چگونه مرورگر خود را ایمن کنیم؟

### ۲- ایمن سازی مرورگر Chrome

به طور کلی با رعایت نکات ایمنی در تمامی مرورگرها میتوان گفت همه ایمن می شوند اما گوگل کروم از ایمن ترین مرورگرهاست که پیشنهاد می شود از آن استفاده کنید. در ادامه به تشریح چند نکته در خصوص ایمن سازی و بهبود عملکرد کروم می پردازیم:

۲-۱- کروم برای اینکه در بحث جستجوی صحیح به شما کمک کند و از هدایت شدن شما به وبسایت‌هایی با نام مشابه ولی محتوای مخرب جلوگیری کند، سرویسی را برای کاربران خود فراهم آورده است که توسط آن می‌توان به وبسایت مورد نظر هدایت شد. از این امکان نیز با رفتن به مسیر **Settings > Language > Enhanced spell check** و فعال نمودن مورد **Enhanced spell check** می‌توان استفاده کرد.

#### Spell check



### تصویر ۷- جستجوی صحیح










۲-۲- شما می‌توانید در مرورگر کروم خود، محتواهایی که ممکن است برای شما بارگذاری شود را مدیریت کنید. به عنوان مثال ممکن است برخی وبسایت‌ها از پلاگین‌های آلوده به محتوای مخرب استفاده کرده باشند. در این صورت کروم شما را از مواجه شدن با چنین وبسایت‌هایی باخبر می‌کند. بنابراین توصیه می‌شود با دنبال کردن مسیر

### : > Settings > Privacy & Security > Site Settings

و غیر فعال کردن موارد مورد نظر خود از جمله JavaScript، PopUp، Location و ... امنیت جستجوهای خود را بالا ببرید.



## چگونه مرورگر خود را ایمن کنیم؟

Permissions	
 Location Sites can ask for your location	▶
 Camera Sites can ask to use your camera	▶
 Microphone Sites can ask to use your microphone	▶
 Notifications Collapse unwanted requests (recommended)	▶
 Embedded content Sites can ask to use info they've saved about you	▶
Additional permissions	
Content	
 Third-party cookies Third-party cookies are blocked	▶
 JavaScript Sites can use JavaScript	▶
 Images Sites can show images	▶
 Pop-ups and redirects Don't allow sites to send pop-ups or use redirects	▶

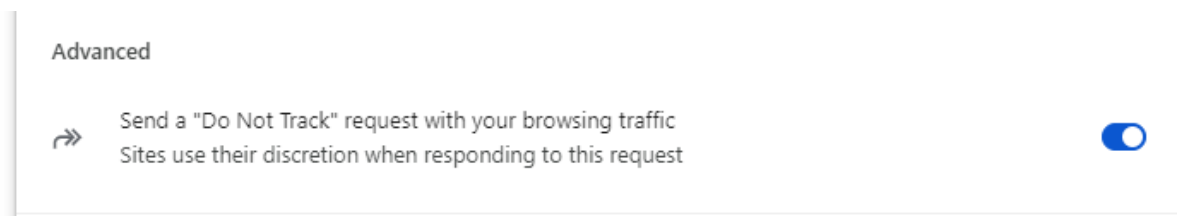
تصویر ۸- مدیریت محتوا





### چگونه مرورگر خود را ایمن کنیم؟

۲-۳- به شما پیشنهاد می‌کنیم برای اینکه وبسایت‌های دیگر جستجوهای شما را دنبال نکنند و از آن‌ها به عنوان منابعی برای تبلیغات خود استفاده نکنند، مسیر **Settings > Privacy & Security > Third-party cookies > Advanced** را دنبال و مورد **Send a "Do Not Track" request with your browsing traffic** را فعال کنید.



### تصویر ۹- مدیریت cookies

با انجام تمام این اقدامات می‌توانید قدمی دیگر در ایجاد فضایی ایمن برای خود بردارید و از ایجاد هرگونه مشکل جلوگیری کنید.