



حریم خصوصی در فایرفاکس

وقتی صحبت از حریم خصوصی می‌شه، مرورگر **فایرفاکس** یک سروگردن از رقباش بالاتره. اما چطوری بهتر ازش استفاده کنیم؟

یکی از موضوع‌های مهمی که باید بهش توجه داشت اثرانگشت (fingerprint) مرورگره. وقتی از سایتی بازدید می‌کنید، مرورگر شما داوطلبانه اطلاعاتی رو به اون‌ها ارسال می‌کنه. این اطلاعات می‌تونه شامل سیستم عامل، ابعاد نمایشگر، نوع مرورگر، منطقه زمانی، و فونت‌هایی باشه که استفاده می‌کنید. حتی افزونه‌های شما در تشکیل این اثرانگشت نقش دارن، و برخلاف چیزی که ممکنه تصور کنید، «بیشتر» لزوماً به معنای بهتر نیست. در نتیجه، در انتخابشون باید دقت کرد.

افزونه‌های مناسب

موقع انتخاب افزونه راجع به کاربرد هرکدوم بخونید، و آگاه باشید که لازم نیست همه افزونه‌های معرفی شده رو نصب کنید. ببینید شرایط شما چی می‌طلبه، و سراغ چیزهایی برید که برای شخص شما مفیدن.

مشاهده لیست افزونه‌های مهم برای حریم خصوصی: privacytools.io/#browser-addons

بررسی وضعیت اثرانگشت مرورگر

سایت بنیاد مرز الکترونیکی (EFF) ابزار خوبی برای سنجش وضعیت اثرانگشت داره: coveryourtracks.eff.org.

The screenshot shows the EFF Cover Your Tracks website. The left sidebar has a green background with the text "COVER YOUR TRACKS" and "TESTING YOUR BROWSER". The main content area on the right has a light beige background. It contains a summary of test results: "Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies." Below this is a table titled "IS YOUR BROWSER:" with three rows: "Blocking tracking ads?" (Yes), "Blocking invisible trackers?" (Yes), and "Protecting you from fingerprinting?" (Your browser has a unique fingerprint).

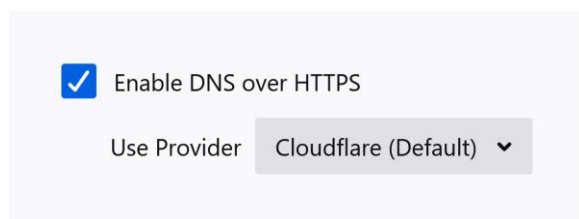
IS YOUR BROWSER:	
Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

ابزار سنجش وضعیت اثرانگشت سایت EFF

پیشنهاد من اینه که درمورد اثرانگشت آگاه باشید، اما دغدغه اصلی شما نباشه. درعوض، سعی کنید با استفاده از افزونه‌های مناسب کنترل جریان اطلاعات و حریم خصوصی خودتون رو به‌دست بگیرید.

تنظیمات فایرفاکس

در قدم بعد، وارد بخش General در تنظیمات فایرفاکس شده، در پایین صفحه Network Settings رو باز کرده، و در پایین پنجره باز شده، اطمینان حاصل کنید گزینه DNS over HTTPS فعاله. (درمورد اهمیتش جستجو کنید.)



وارد بخش Privacy & Security در تنظیمات فایرفاکس بشید. اینجا گزینه‌های بیشتری برای بررسی و انتخاب دارید.

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](#)

- ☐ 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](#)

غیرفعال کردن ارسال داده‌های فنی به فایرفاکس

General Certificates

☒ Query OCSP responder servers to confirm the current validity of certificates [View Certificates...](#)

[Security Devices...](#)

Home

Search

Privacy & Security **HTTPS-Only Mode**

Sync

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS. [Learn more](#)

☒ Enable HTTPS-Only Mode in all windows

☐ Enable HTTPS-Only Mode in private windows only

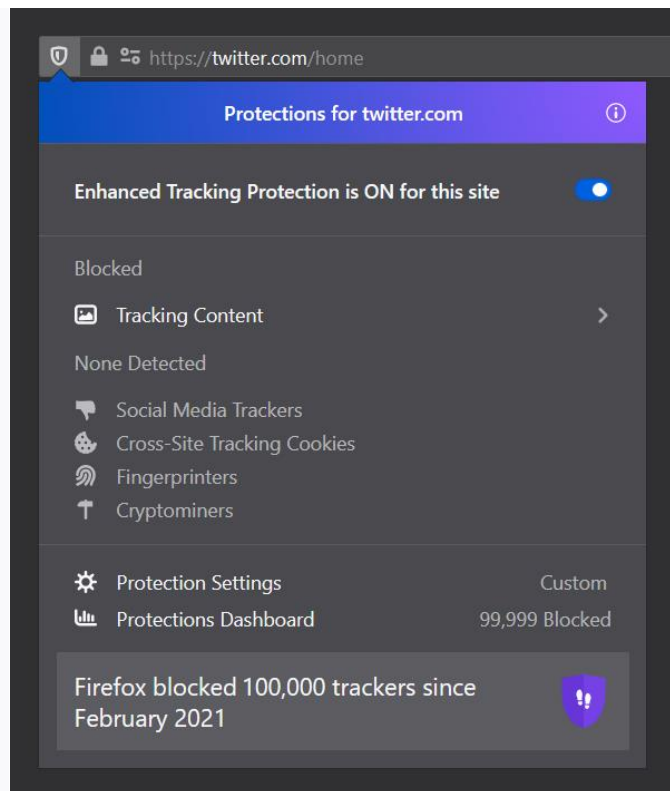
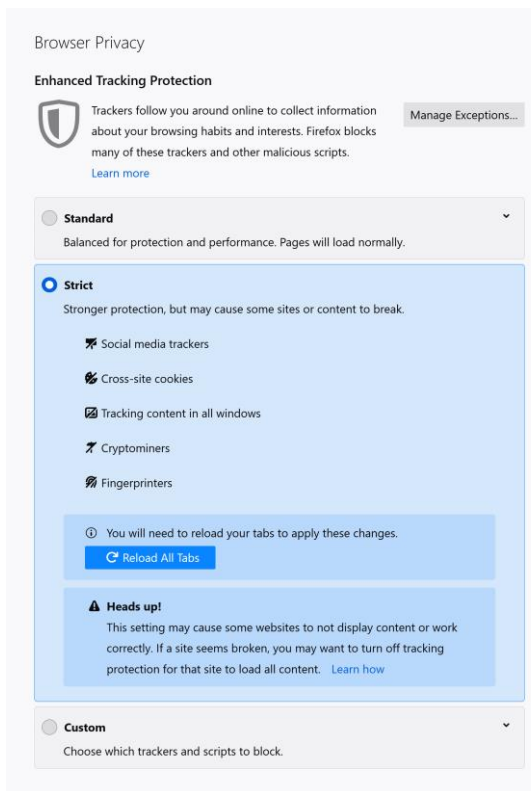
☐ Don't enable HTTPS-Only Mode

Extensions & Themes

Firefox Support

فعال کردن حالت HTTPS-Only

قبل از پرداختن به قابلیت Enhanced Tracking Protection، ابتدا اطمینان حاصل کنید هیچ داده‌ای برای فایرفاکس ارسال نمی‌کنید و همچنین حالت HTTPS-Only فعاله.



حالت Strict برای بیشترین حریم خصوصی ممکن

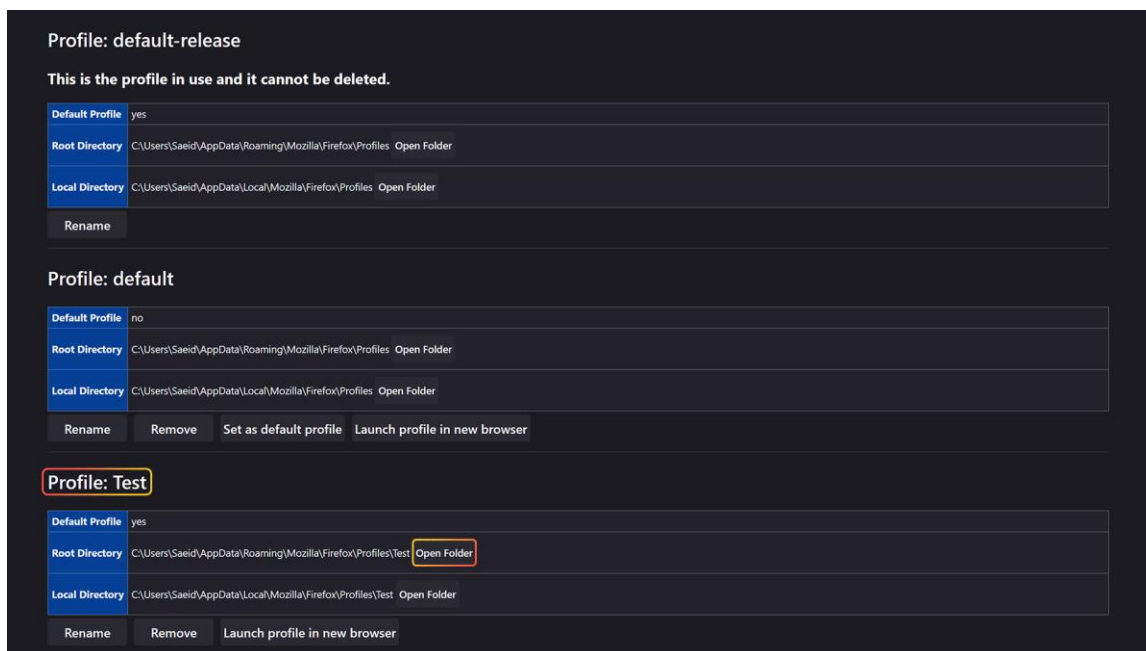
گزینه Strict بیشترین حریم خصوصی رو ارائه می‌ده، اما ممکنه باعث بشه بعضی سایت‌ها از کار بی‌افتن. بررسی کنید و ببینید چه چیزی برای شما بهتره، و اگه نمی‌دونستید، حتماً پیرسید. درضمن، حتی اگه از حالت Strict استفاده کنید، می‌تونید اون رو برای سایت‌های خاصی غیرفعال کنید.

جلوگیری از نشت داده

در مرحله بعد می‌خوایم جلوی نشت داده (data leak) رو بگیریم. ابتدا به یک روش ساده می‌پردازیم و سپس به یک روش تخصصی‌تر.

راه حل ساده

وارد سایت ffprofile.com شده، به بخش Privacy رفته، و روی گزینه Save در انتها بزنید. ترتیب چیزهای مهم رو می‌ده. اگه کنجکاو بودید، بخش‌های دیگه‌ش رو هم ببینید. سپس، به بخش Finish رفته و profile.zip رو دانلود کنید.



ایجاد پروفایل جدید با زدن روی Create a New Profile و سپس بازکردن پوشه Root Directory

در مرحله بعد، در نوار آدرس بنویسید `about:profile` و `enter` بزنید. با انتخاب گزینه `Create a New Profile` یک پروفایل جدید ایجاد کرده و پوشه `Root Directory` مربوط به اون رو باز کنید، مثل تصویر بالا. سپس، مرورگر رو ببندید. فایل های موجود در پوشه **پروفایل جدید** رو پاک کرده و محتوای `profile.zip` رو اونجا از حالت فشرده خارج کنید. با بازکردن مجدد فایرفاکس، مرورگر از پروفایل جدید پیروی خواهد کرد. درضمن، همیشه می تونید با رفتن به `about:profile` به پروفایل قبلی برگردید. در انتها، افزونه های مورد نیاز رو نصب کرده و شخصی سازی های مورد نیاز رو انجام بدید.

راه حل تخصصی

یکی از نشت های مهم WebRTC است. در موردش جستجو کنید و بخونید. اینجا می خوایم به طور کامل غیرفعالش کنیم.

در نوار آدرس مرورگر بنویسید `about:config` و کلید `enter` رو بزنید؛ از هشدار بگذرید، و مواردی رو که در ادامه می بینید جستجو کنید و تغییر بدید.

☐ Show only modified preferences

media.peerconnection.enabled	false		5
media.peerconnection.turn.disable	true		5
media.peerconnection.use_document_iceservers	false		5
media.peerconnection.video.enabled	false		5
media.peerconnection.identity.enabled	false		5
media.peerconnection.identity.timeout	1		5
media.peerconnection.dtmf.enabled	false		5
media.peerconnection.video.vp9_enabled	false		5

1. media.peerconnection.enabled = false
2. media.peerconnection.turn.disable = true
3. media.peerconnection.use_document_iceservers = false
4. media.peerconnection.video.enabled = false
5. media.peerconnection.identity.enabled = false
6. media.peerconnection.identity.timeout = 1
7. media.peerconnection.dtmf.enabled = false
8. media.peerconnection.video.vp9_enabled = false

برای اطلاعات بیشتر در مورد این موارد و اینکه چرا بعضی رو غیرفعال و بعضی دیگه رو فعال می کنیم، [این مطلب](#) رو بخونید.



ابزارهای کارآمد فایرفاکس

فایرفاکس ابزارهای قدرتمندی دارد، بعضی‌هاشون منحصر به فرد و مختص همین مرورگر. در اینجا قراره به سه تا از مهم‌ترین‌ها و دوتا از جالب‌ترین‌ها اشاره کنیم.

اطلاع از درز اطلاعات مهم با Firefox Monitor

یکی از چیزهایی که همیشه در مورد فایرفاکس موردتحمین قرار گرفته توجهش به موضوع حریم خصوصی و اینترنت آزاده. ابزار Firefox Monitor تلفیق سایت [Have I Been Pwned](#) با این مرورگره. طی سالیان، بارها نقض داده (data breach) اتفاق افتاده، اون هم در ابعاد بزرگ، و اطلاعات مهم کاربرها فاش شده، از جمله [هک اخیر پلتفرم توئیچ](#).

این ابزار به شما اجازه می‌ده آدرس ایمیلتون رو وارد کنید، و به شما خواهد گفت اطلاعاتتون لو رفته یا نه—کی، کجا، و دقیقاً چه اطلاعاتی. شما در مقابل می‌تونید هرچه زودتر در راستای ارتقای امنیت حساب‌هاتون قدم بردارید قبل از اینکه دیر بشه.

امتحانش کنید: monitor.firefox.com



حساب خود را مدیریت کنید

وارد سایت Relay شده تا آدرس‌هایی را که ساخته‌اید پایش کنید. در صورتی که یکی از آدرس‌ها هرزنامه یا پیام‌های ناخواسته دریافت می‌کند، می‌توانید دریافت پیام از آن را متوقف و یا آن را به کلی حذف کنید.



آدرس مستعار جدید بسازید

هنگام وب‌گردی، آیکون Relay را درون فرم‌های ثبت‌نام خواهید دید. آن را انتخاب کرده تا یک آدرس جدید و تصادفی تولید کنید که انتهای آن با @relay.firefox.com تمام می‌شود. Relay پیام‌های دریافتی شما را به آدرس ایمیل اصلی شما هدایت (forward) خواهد کرد.



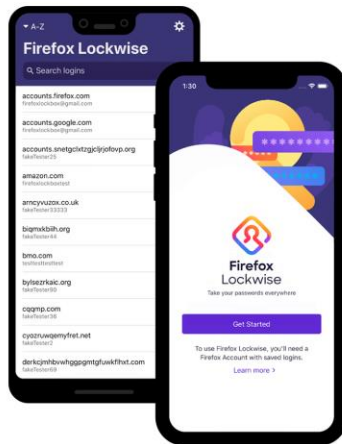
افزونه را نصب کنید

افزونه Relay را دانلود و نصب کنید. روی آیکونی که در گوشه سمت راست نوار ابزار مرورگر پدیدار می‌شود کلیک کرده تا به صفحه ورود منتقل شوید. برای شروع به استفاده، وارد حساب فایرفاکس خود شوید.

حفاظت از آدرس ایمیل با Firefox Relay

ابزار Firefox Relay به شما این امکان رو می‌ده آدرس‌های تصادفی تولید و هنگام ثبت‌نام در سایت‌ها، به جای استفاده از آدرس ایمیل اصلی تون، از اون‌ها استفاده کنید. با این کار، از هویت واقعی تون محافظت می‌کنید.

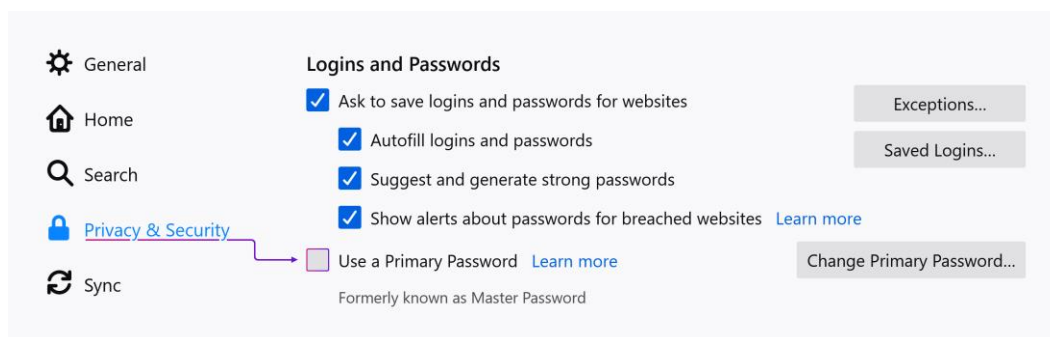
امتحانش کنید: relay.firefox.com



مدیریت گذرواژه‌ها با Firefox Lockwise

ابزار Firefox Lockwise عهده‌دار مدیریت گذرواژه‌های شماست. حین ثبت‌نام در سایت‌ها می‌تونه گذرواژه تولید (generate) و فیلد مربوطه رو خودکار پر کنه، و از شما می‌پرسه می‌خواید ذخیره‌ش کنید یا نه. با داشتن حساب فایرفاکس می‌تونید رمزها رو SYNC کرده و در دستگاه‌های مختلف بهشون دسترسی داشته باشید. درنظر داشته باشید که به‌طورکامل بهش متکی نشید. درضمن، ابزارهای بهتر و تخصصی‌تری برای مدیریت گذرواژه وجود دارن: [اینجا](#).

توجه مهم: اگه از حساب فایرفاکس برای نگهداری رمزها استفاده می‌کنید، حتماً احراز هویت دوعاملی رو فعال کنید. درغیراین‌صورت، تنها چیزی که بین یک هکر و کل رمزهای شما قرار گرفته تک‌رمز حساب فایرفاکس شماست.

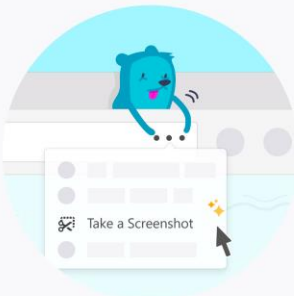


درضمن، هر کسی که به کامپیوتر شما دسترسی داشته باشه، می‌تونه رمزهای شما رو ببینه. مهمه که Primary Password رو فعال کنید. با داشتنش، با هر بار بازکردن مرورگر ازتون می‌خواد اون رو وارد کنید. حواستون باشه رمز خوبی انتخاب کنید و فراموشش نکنید چون دسترسی‌تون رو به رمزها از دست خواهید داد.

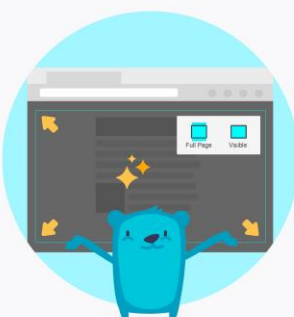
گرفتن اسکرین شات با Firefox Screenshots

ابزار پیشرفته Firefox Screenshots نه تنها اسکرین شات گرفتن رو آسون کرده بلکه بهش لذت بخشیده. کافیه یک بار امتحانش کنید.

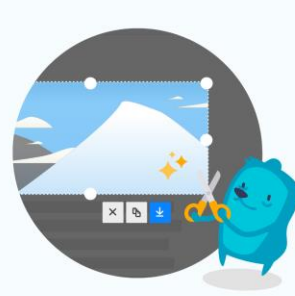
در انتهای نوار آدرس، روی سه نقطه (...) بزنید، و گزینه Take a Screenshot رو انتخاب کنید. منوی اسکرین شات روی پنجره فعلی مرورگر شما ظاهر می شه. برای سهولت بیشتر از کلیدهای میانبر Ctrl + Shift + S استفاده کنید.



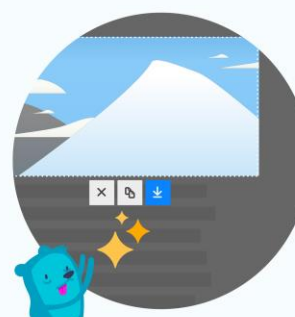
از گزینه های بالا سمت راست می تونید برای ثبت تصویر تمام صفحه استفاده کنید. گزینه Visible فضایی رو که در پنجره می بینید ثبت می کنه — بدون اسکرول کردن — و Full Page تمام صفحه رو، از بالا تا پایین.



در جایی از صفحه کلیک کرده و بکشید (click and drag) تا فضای مورد نظر رو ثبت کنید. یا نشانگر ماوس رو روی فضای مورد نظر ببرید، و اسکرین شات فایرفاکس خودکار اون قسمت رو تشخیص می ده.



بعد از ثبت تصویر، می تونید اون رو در کلیپ بورد کپی یا مستقیم دانلود کنید. اسکرین شات گرفتن هرگز آسون تر نبوده.



شخصی سازی فایرفاکس

فایرفاکس به قابلیت های شخصی سازی اش معروفه. اگه ظاهر مرورگری که هر روز ازش استفاده می کنید برای شما اهمیت داره، فکر می کنم از این امکان لذت خواهید برد. درضمن، کلی قالب (theme) از قبل ساخته شده هست که می تونید از بینشون انتخاب کنید.

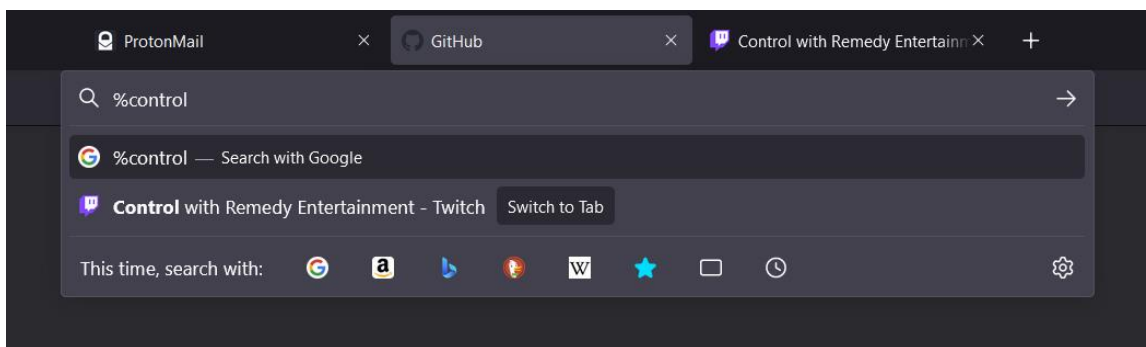
امتحان کنید: color.firefox.com



ترفندهای فایرفاکس

اگر کارایی هدف شماست، سعی می‌کنید روش‌های استفاده بهتر از هر ابزاری رو یاد بگیرید. کارایی برای من یعنی صرفه‌جویی در زمانم، اما، جدا از اون، لذتی که از انجام بهینه کارها می‌برم انگیزه‌بخشه. در این مطلب یاد خواهیم گرفت چطور حرفه‌ای‌تر از فایرفاکس استفاده کنیم.

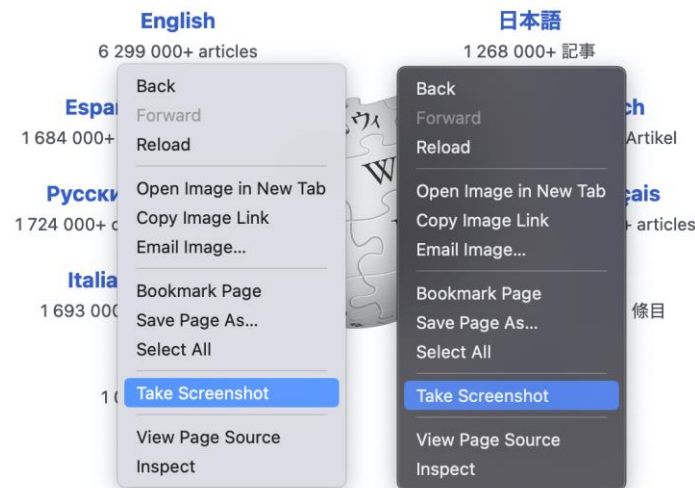
جستجو در تب‌ها



اگر شما هم مثل من کلی تب باز می‌کنید و بعد پیدا کردن یک تب خاص مثل پیدا کردن یک سوزن در انبار کاه می‌شه، کافیه در نوار آدرس یک علامت درصد (%) بذارید. حالا می‌تونید بین تب‌های باز فایرفاکس (حتی در پنجره‌های مختلف) جستجو کنید.

درضمن، با استفاده از علامت‌های ستاره (*) و هشتک (^) می‌تونید به ترتیب در بوکمارک‌ها و تاریخچه مرورگرتون جستجو کنید. برای منی که محتواهای خوندنی و دیدنی‌ام رو با بوکمارک مدیریت می‌کنم، استفاده از این ترفند فوق‌العاده مفیده. یک مرحله فراتر؟ برای هر بوکمارک یک keyword تعیین کنید. این کلیدواژه می‌تونه به کوچکی یک حرف یا عدد باشه، که با نوشتنش و زدن کلید enter بوکمارک مربوطه برای شما باز خواهد شد. با استفاده متوالی از این‌ها ملکه ذهنتون خواهند شد.

اسکرین شات



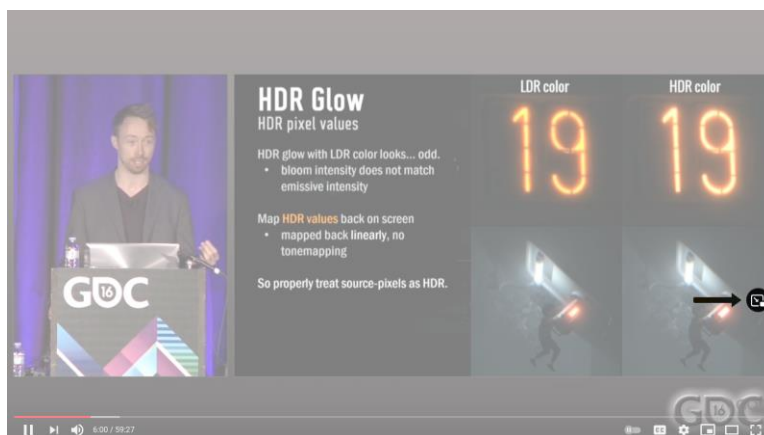
بالا تر به قابلیت پیشرفته اسکرین شات این مرورگر پرداختیم. در هر صفحه‌ای که باشید، کافیه راست کلیک کرده و گزینه Take Screenshot رو انتخاب کنید یا، اگه مثل من بیشتر اوقات دستتون روی صفحه کلیده، کلیدهای میان‌بر Ctrl + Shift + S رو فشار بدید.

بازیابی یک تب بسته شده

حتماً پیش اومده که تپی رو به اشتباه ببینید. چطور می‌تونید تب‌های بسته شده رو مجدد باز کنید؟ به راحتی آب خوردن: کافیه از میان‌بر Ctrl + Shift + T استفاده کنید.

توجه کنید که اگه کاربر مک هستید، کافیه Ctrl رو با کلید Command جایگزین کنید.

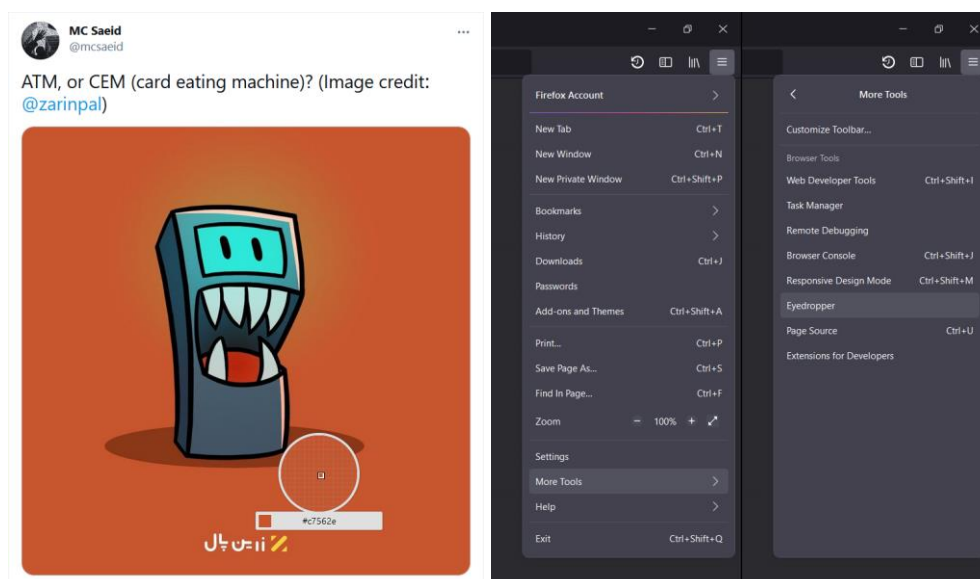
انجام هم‌زمان چند کار



یکی از چیزهایی که در صرفه‌جویی زمان کمک زیادی به من می‌کنه قابلیت تصویر در تصویر (picture-in-picture) فایرفاکس—بسیار محبوب، بسیار کاربردی. این یعنی می‌تونم ویدئو ببینم و هم‌زمان کار هم بکنم. با ماوس روی ویدئو رفته و روی آیکون تصویر در تصویر بزنید.

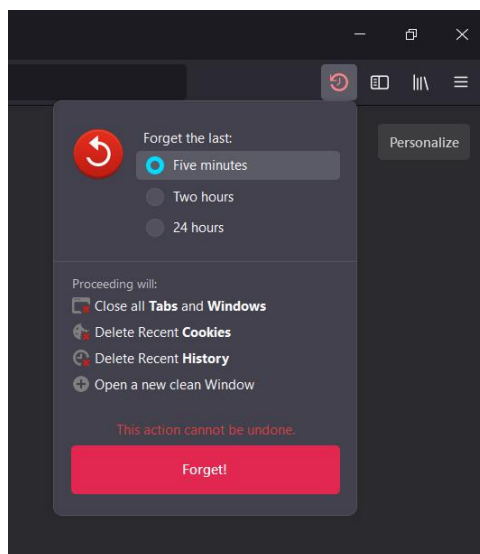
یافتن رنگ دقیق با قطره‌چکان درون مرورگر

دنیای وب پره از رنگ‌های مختلف و زیبا، و هر رنگی یک کد هگزادسیمال منحصر به فرد داره. قابلیت Eyedropper، برای اون دسته که اهل طراحی‌ان، می‌تونه بسیار کاربردی باشه. از منوی اصلی سمت راست More Tools → Eyedropper رو انتخاب کنید.



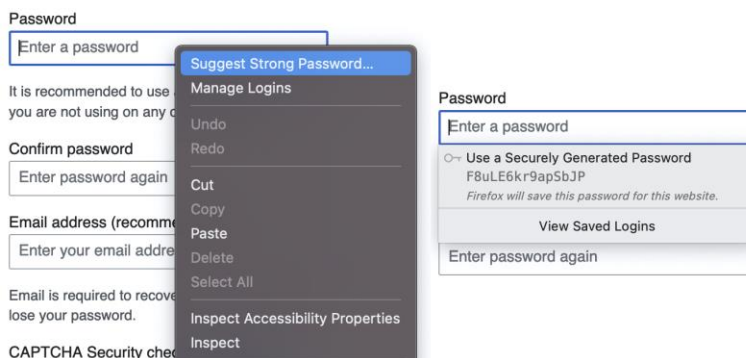
پاک کردن سریع تاریخچه یا، به قولی، fuggedaboutit!

زمانی هست که می‌خواید تاریخچه وب‌گردی رو خیلی سریع پاک کنید. ابزار Forget این کار رو از همیشه آسون‌تر کرده.



به More Tools → Customize Toolbar رفته، آیکون Forget رو پیدا کرده، و اون رو به نوار ابزار مرورگر اضافه کنید.

پیشنهاد گذرواژه‌های قوی



با کلیک روی فیلد گذرواژه یا راست کلیک و انتخاب Suggest Strong Password، فایرفاکس می‌تونه گذرواژه‌های به نسبت قوی و خوبی رو پیشنهاد بده. فراموش نکنید که Primary Password هم تعیین کنید تا از گذرواژه‌هاتون محافظت کنه. درضمن، این راهنما برگرفته از مطلب جامع‌تر [ترفندهای مخفی فایرفاکس](#). چهار ترفند دیگه هم وجود داره، که پیشنهاد می‌کنم برای آشنایی باهاشون مقاله مربوطه رو بخونید.

راهنماهای مرتبط



معرفی ProtonMail: حریم خصوصی و امنیت



حریم خصوصی در عصر دیجیتال



راهنمای جامع نرم افزار PGP



رمزنگاری کلید عمومی RSA

