



## حریم خصوصی در عصر دیجیتال

به همراه راهنمای عملی به کارگیری ابزارهای موجود

## مقدمه

با واژه حریم خصوصی غریبه نیستیم. مدافع‌های زیادی داره، اهمیت و نیازش هنوز برای عموم روشن نیست، و از دید بسیاری برابره با پنهان کردن چیزهای بد. جوامع و حکومت‌های مدرن مدام درتلاش این تصویر دورازحقیقت رو در ذهن افراد نهادینه کنن. اینجا لازمه از خودتون پرسید چرا.

این فهرست، تهیه شده توسط [6102bitcoin](#)، برای اون دسته از افراد که به اهمیت موضوع واقفن و دوست دارن آگاهانه‌تر، با دغدغه کمتر نسبت به نقض حریم خصوصی و آزادی شون، در عصر دیجیتال زندگی کنن. راجع به هر مورد و دلیل وجودش در لیست فکر کنید. دوست دارید یک مرحله فراتر برید؟ بسیار عالی؛ راجع به هرکدوم جداگونه تحقیق کنید.

ام‌سی سعید

پاییز ۱۴۰۰

## ۱. از لینوکس استفاده کنید



مشاهده ویدئوی معرفی سیستم عامل Tails در توئیتر؛ کاری از استودیو ویویدو، با همکاری نیما فاطمی

## ۲. از گوگل اجتناب کنید (چرا؟)

در عوض، از [DuckDuckGo](#) استفاده کنید.

## ۳. از تلفن های burner استفاده کنید

این مورد به سادگی خرید یک تلفن ارزون قیمت و سیم کارت بدون هویت نیست. نحوه خرید و پرداخت شما—در کنار عوامل دیگه—مهمه. [این ویدئو](#)، با ته‌مایه طنز، شما رو با ذهنیت موردنیاز برای این کار آشنا می‌کنه، و می‌تونه الهام‌بخش باشه.

## ۴. از مسدودکننده تبلیغات (ad blocker) استفاده کنید

هدف تنها این نیست که کمتر تبلیغ ببینید. افزونه uBlock Origin رو پیشنهاد می‌کنم. جلوتر در مورد ابزارها و افزونه‌های دیگه‌ای که می‌تونید همراه با مرورگرتون استفاده کنید صحبت خواهیم کرد.

👉 نصب افزونه فایرفاکس

## ۵. از وی‌پی‌ان استفاده کنید

در وهله اول، اطمینان حاصل کنید از وی‌پی‌انی استفاده می‌کنید که قابل اعتماد است. آگه از سایت‌های فارسی زبان داخلی اشتراک تهیه می‌کنید، نیازه در این تصمیم بازیابی کنید.



**س** آیا وی‌پی‌ان‌ها/فیلترشکن‌هایی که در ایران فروخته می‌شوند، قابل اطمینان هستند؟

**ج** خیر، این فیلترشکن‌ها به هیچ وجه قابل اطمینان نیستند. مشخص نیست کدام شرکت و با چه سیاست‌هایی این سرویس‌ها را راه‌اندازی کرده و همچنین معلوم نیست که سرورهای این فیلترشکن‌ها تحت کدام حوزه قضایی فعالیت می‌کنند. شما با پرداخت هزینه خرید از طریق کارت بانکی خود، این امکان را به سازندگان این فیلترشکن‌ها می‌دهید که فعالیت‌های آنلاین شما را به هویت اصلی بانکی شما ربط دهند.

Paskoocheh.com پس‌کوچه  
@Paskoocheh

آیا وی‌پی‌ان‌ها/فیلترشکن‌هایی که در ایران فروخته می‌شوند، قابل اطمینان هستند؟

سرویس‌دهنده وی‌پی‌ان شما می‌تونه ببینه از چه سایت‌هایی بازدید می‌کنید. (تصویر: ProtonVPN)

<b>MYTH</b>	With a VPN, you'll be anonymous online.
<b>FACT</b>	Full anonymity with a VPN service is technically impossible.

در وهله دوم، اطمینان حاصل کنید وی‌پی‌انی که استفاده می‌کنید نشت (leak) نداشته. درضمن، در نظر داشته باشید منطقه زمانی شما به راحتی قابل تشخیص است.

بررسی نشت آی‌پی

بررسی نشت WebRTC؛ اطلاعات بیشتر

بررسی منطقه زمانی

## ۶. از تور استفاده کنید



معرفی و آموزش راه اندازی سرویس تور در یوتیوب

معرفی سرویس تور در یوتیوب

در ویدئوی بالا، کاری از **استودیو کج آرت** با همکاری نیما فاطمی، از اعضای اصلی تیم **پروژه تور**، کوتاه با کاربرد این سرویس ارزشمند آشنا می‌شید. من هم در ویدئویی مفصل‌تر به معرفی و استفاده از آن می‌پردازم.

## ۷. آگه از شخص ناشناسی لینک دریافت کردید، بازش نکنید

اینترنت جای خطرناکیه. با احتیاط بیشتری رفت‌وآمد کنید. درمقابل، آگه در موقعیت ارسال پیام هستید و شخص مقابل شما رو نمی‌شناسه، تا حد امکان از قراردادن لینک و ضمیمه اجتناب کنید. به‌قولی، آداب و رسوم اینترنتی (netiquette) رو رعایت کنید.

## ۸. به تماس‌های ناشناس جواب ندید

به‌شخصه، سال‌هاست که این روش رو پیش گرفته‌م. یک ادب خوب، از دید من، اینه که همیشه خودتون رو در نقطه مقابل هم قرار بدید. آگه قراره با کسی تماس بگیرید که شما رو نمی‌شناسه، مؤدبانه‌ست که قبلش خبر بدید، حتی با یک پیام. اون شخص موظف به پاسخ دادن به تماس شما نیست.

## ۹. از روش‌های مناسب برای برقراری ارتباط استفاده کنید

از **Signal**، **Keybase**، و نرم‌افزارهایی استفاده کنید که رمزنگاری سرتاسر (end-to-end encryption) دارن. بیشتر مکالمه‌های روزمره من در فضای E2EE اتفاق می‌افته. درمورد اهمیت رمزنگاری در مکالمه‌ها **اینجا** بخونید.

برای مثال، توئیتر مکان مناسبی برای داشتن یک مکالمه مهم نیست. پیام‌های ردوبدل شده نه E2EE هستن و نه ازبین می‌رن. اطلاعاتی که در پیام خصوصی با دوستی به اشتراک می‌ذارید یا عکسی که برای یک غریبه می‌فرستید نه تنها قابل حذف نیستن بلکه در صورت دسترسی شخص سومی به حساب شما یا دیگری می‌تونن خطرناک هم باشن.

در نتیجه، همیشه سعی کنید مکالمه رو به کانال امن تری سوق بدید.

یکی از روش‌هایی که کنترل بیشتری روی مکالمه در توئیتر (و پلتفرم‌های دیگه) به شما می‌ده استفاده از ابزار **Pastebin** است. می‌تونید پیامی رو نوشته و انقضای اون رو **burn after read** قرار بدید تا یک بار مصرف باشه.

## ۱۰. از شبکه‌های اجتماعی با نام و هویت واقعی تون استفاده نکنید

شبه‌ناشناسی (pseudonymity) مزیت‌های خودش رو داره—اگه به درستی پیاده بشه—و می‌تونه در حفظ حریم خصوصی شما بسیار مؤثر باشه.

ممکنه براتون جالب باشه که «مقاله‌های فدرالیست» با نام مستعار پوبلیوس (Publius) امضا و منتشر شدن.

## ۱۱. حواستون به میکروفون‌های همیشه فعال (always-on) باشه

شاید همه خونه هوشمند نداشته باشن، اما خیلی‌ها از Siri، Google Assistant، و ابزارهای مشابه استفاده می‌کنن. همیشه نمی‌شه سهولت و حریم خصوصی رو در کنار هم داشت. این موضوع که همه دستگاه‌ها مون می‌تونن به ما گوش بدن واقعیتی ترسناک اما در حال اتفاقه.

## ۱۲. تا حد امکان از پول نقد استفاده کنید

«حریم خصوصی این روزها یک کالای لوکس است که هر روز گران‌تر می‌شود.» — کتاب کوچک بیت کوین

در مورد پول، کارکردش، و ضعف‌هاش در فصل اول این کتاب فوق‌العاده بخونید یا بشنوید.

### ۱۳. عکس آپلود نکنید

هوشمند عمل کنید. قبل از ارسال هر چیزی روی اینترنت به عواقب احتمالی اش فکر کنید. چیزی رو نشر ندید که در آینده بخواید به حذفش فکر کنید.

### ۱۴. از گذرواژه‌های قوی استفاده کنید

از چیزهایی مثل 1Password و LastPass—یا iCloud Keychain در صورتی که کاربر آی‌اواس هستید—دوری کنید. در مقابل، از نرم‌افزارهای متن‌باز و آزادی مثل KeePassXC یا Bitwarden استفاده کنید.

👉 اطلاعات بیشتر در مورد نرم‌افزارهای مدیریت گذرواژه

### ۱۵. از احراز هویت دو عاملی (two-factor authentication) استفاده کنید

در فعال کردن 2FA شک نکنید. لزومی به استفاده از Google Authenticator نیست؛ جایگزین‌های متن‌باز رو امتحان کنید، مثل andOTP. هرگز از روش پیامک (SMS) استفاده نکنید چون از امنیت کافی برخوردار نیست.

### ۱۶. وب‌کم (یا دوربین) رو پوشونده، غیرفعال کرده، یا در صورت امکان در بیارید؛ میکروفون رو قطع یا غیرفعال کرده یا به کلی جدا کنید

برای اینکه اهمیت این موضوع رو بهتر درک کنید، مستند کوتاه [State of Surveillance](#) (دولت نظارت) رو ببینید.

فرقی نمی‌کنه اگه دسترسی‌های موقعیت مکانی رو غیرفعال کرده باشید، فرقی نمی‌کنه به اینترنت و وای‌فای متصل باشید یا نه؛ تا زمانی که تلفن همراه شما روشنه، در شبکه حضور دارید.

## ۱۷. از اینترنت عمومی استفاده نکنید

دفعه بعد که خواستید به وای فای مجانی کافه مورد علاقه تون وصل بشید، بیشتر فکر کنید.



مشاهده ویدئو در توئیتر

## ۱۸. اطلاعات شخصی خودتون رو در اختیار عموم قرار ندید

علاوه بر اینکه لزومی نداره افراد، به خصوص غریبه‌ها، راجع به جزئی ترین چیزهای زندگی شما بدونن، با به اشتراک گذاری (یا درز ناخواسته) چنین اطلاعاتی شما یکی از بزرگ ترین ریسک های آنلاین رو متحمل می شید.



مشاهده ویدئو در توئیتر



اگر غریبه‌ای رو در خیابون ببینید و از شما در مورد اطلاعات شخصی تون سؤال کنه، چه جوابی بهش می‌دید؟ آیا نام کامل، تاریخ تولد، شماره، محل سکونت، و سابقه کاری تون رو در اختیارش می‌ذارید، یا مردد می‌شید و قبلش فکر می‌کنید؟ به همین ترتیب، اگر چیزی در اینترنت منتشر می‌کنید، هرکسی می‌تونه اون رو ببینه.

این می‌تونه امتدادی از نکته بالاتر در مورد انتشار عکس باشه: حتی اگر عکس یا اسکرین‌شاتی به اشتراک می‌ذارید، توجه داشته باشید که اطلاعات مهم رو از معرض دید پاک کنید. اطمینان حاصل کنید که این کار رو درست انجام داده‌اید. این [مقاله](#) تلنگر خوبییه.

قبل از پرداختن به موضوع بعدی و برای اینکه استراحت کوتاهی هم کرده باشیم، می‌خوام اشاره کنم که من می‌دونم از دید کسی که دغدغه مشابهی نداره، این‌ها ممکنه شعارگونه به نظر بیان، اما من به همه موارد لیست معتقدم، و تلاش کرده‌م و می‌کنم بهشون پایبند باشم.

این‌ها همه پیشنهاد: اجباری در انجام هیچ‌کدوم نیست. هرکسی آزاده هرطور که علاقه داره زندگی کنه، و من به تصمیم همه افراد احترام می‌ذارم. اگر دوست دارید آزادانه در شبکه‌های اجتماعی سیر کنید، بدون دغدغه عکس و ویدئو منتشر کنید، و نگران موضوع‌های مطرح‌شده در این مقاله نباشید، تشویقتون هم می‌کنم.

به اعتقاد من، از دو چیز باید به‌دور بود: حاشیه و تعصب. همه عاقل و بالغ هستیم، و می‌تونیم برای خودمون تصمیم بگیریم. ضمن اینکه تجربه من نشون داده شما نمی‌تونید کسی رو مجبور به انجام کاری بکنید. اون شخص خودش باید به درک از اون نیاز برسه. تا اون زمان، کاری از دست شما ساخته نیست.

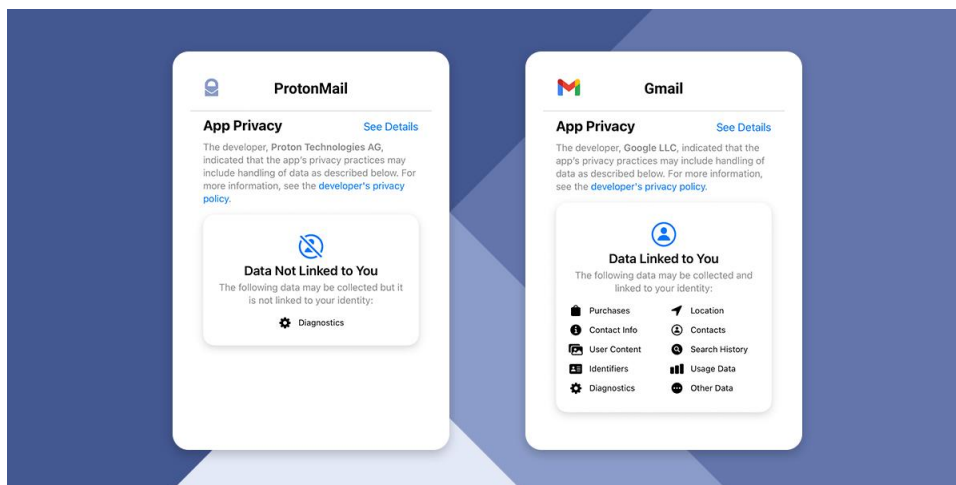
## ۱۹. از ایمیل‌های موقت استفاده کنید

ایمیل واقعاً راه ارتباطی امنی نیست. جلوتر بعد به نشت داده اشاره می‌کنم، و خواهید دید که درز اطلاعات چطور می‌تونه امنیت و حریم خصوصی شما رو به‌خطر بی‌اندازه.

👉 سرویس [Temp Mail](#) یا [Email on Deck](#)

می‌تونید سرویس‌های دیگه رو جستجو کنید.

اما آگه به آدرس ایمیل نیاز دارید، از سرویس‌هایی استفاده کنید که به حریم خصوصی شما احترام می‌ذارن. جی‌میل، یاهو، و غیره رو کنار بذارید. (آگه نیازه، تحقیق کنید چرا باید کنارشون بذارید.) پروتون‌میل یکی از گزینه‌های خوبه که می‌تونید بهش مهاجرت کنید.



مقایسه حریم خصوصی اپ‌های پروتون‌میل و جی‌میل در آی‌اواس (تصویر: ProtonMail)

در مقاله‌ای مجزا به معرفی و بررسی سرویس پروتون‌میل پرداخته شده. آگه قصد دارید بررسی‌اش کنید، می‌تونید شروع خوبی باشه. برای مطالعه‌ش به صفحه‌شونزده همین راهنما رجوع کنید.

## ۲۰. از فایرفاکس استفاده کنید

مهاجرت سخت اما ضروریه. فرقی نمی‌کنه کاربر ویندوز هستید، مک، یا لینوکس؛ فایرفاکس برای هر سه موجوده. نگران بوکم‌ها و لاگین‌ها تون هستید؟ به راحتی می‌تونید از هر مرورگری به فایرفاکس انتقال بدید. آگه هنوز از کروم و سافاری استفاده می‌کنید، وقتشه قدم بعدی رو بردارید.



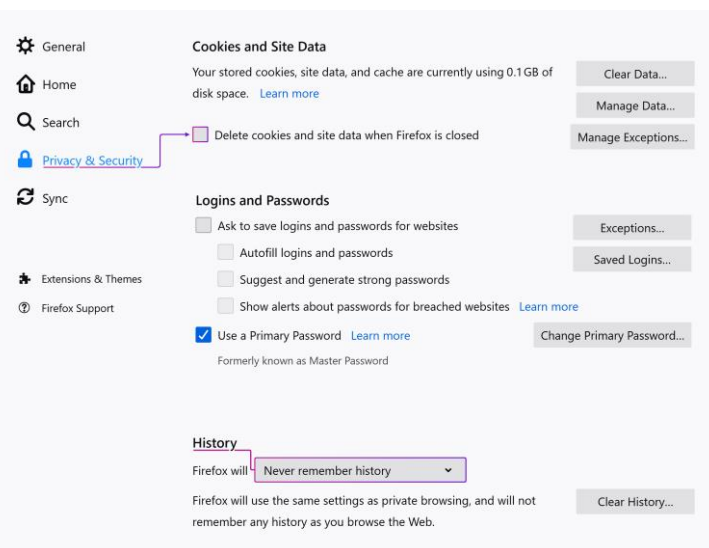
نرم افزارهای جایگزین برای حفظ بهتر و بیشتر حریم خصوصی (تصویر: Bitcoin Q+A)

در مقاله‌ای مجزا به معرفی نکات حریم خصوصی، ابزارها، و ترفندهای فایرفاکس پرداخته شده. برای مطالعه‌ش به صفحه سی و پنج همین راهنما رجوع کنید.



## ۲۱. تاریخچه وبگردی و کوکی‌ها رو خودکار پاک کنید

در مورد کوکی‌ها بخونید. کارشون؟ به خاطر سپردن تنظیمات، اطلاعات ورود، اطلاعات وارد شده در فرم‌ها، و غیره. به لطف کوکی‌ها، با بستن و بازکردن مرورگر نیازی به ورود دوباره در سایت‌ها نیست. اما کوکی‌هایی هم هستن که شما رو دنبال (track) می‌کنن.



افزونه **Cookie AutoDelete** می‌تونه کار شما رو راحت کنه. پیشنهاد می‌کنم سری به تنظیمات حریم خصوصی و امنیت مرورگر هم بزنید.

## ۲۲. آگه قدیمیه و امتحان خودش رو پس داده، مثل PGP، ازش استفاده کنید؛ آگه تازه‌ست و پرطرفدار، احتیاط کنید

در دو مقاله مجزا به رمزنگاری کلید عمومی RSA و آموزش جامع نرم‌افزار PGP پرداخته شده. مقاله اول پیش‌نیاز دومیه. پیشنهاد می‌شه از [اینجا](#) مطالعه کنید.

## ۲۳. به طور مداوم سیستم عامل دستگاهتون رو حذف و دوباره نصب کنید

هارد دیسک‌ها و اس‌اس‌دی‌ها رو قبل از دورانداختن حتماً به صورت فیزیکی از بین ببرید.



سکانسی در سریال مستر ربات؛ الیوت، شخصیت اصلی، تمام حافظه‌های ذخیره‌سازی خودش رو از بین می‌بره

## ۲۴. تلفن همراهتون رو در کشو قرار بدید

خاموش بودن به معنای خاموشی کامل نیست.

## ۲۵. هرگز حافظه‌های فلش ناشناخته رو به دستگاهتون وصل نکنید



Ben Wood  
@benwood

Got myself a USB condom... Getting increasingly nervous about what could happen to my data when I plug into a random USB socket on a plane, train, car...



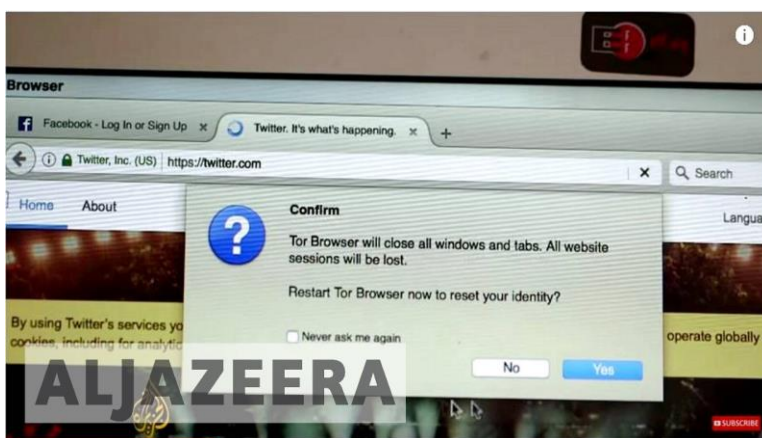
روشی جالب جهت محافظت از حافظه‌های فلش (تصویر: توئیتر)

## ۲۶. کتاب بخونید (ترجیحاً فیزیکی تا دیجیتال)

کتاب و مقاله بخونید، و سعی کنید مدام به دانشتون در این زمینه (و هر زمینه مهم دیگه‌ای) اضافه کنید. این مهم‌ترین اصله.

## ۲۷. تا حد امکان از پیامک و تلفن استفاده نکنید

یکی از نکات جالبی که در ویدئوی زیر بهش اشاره می‌شه استفاده از دستگاهی مثل آی‌پاد به جای تلفن همراه. از امکانات یک گوشی هوشمند بهره‌مندید، منهای قابلیت برقراری تماس و ارسال پیامک. ویدئو رو برای اطلاعات بیشتر ببینید.



مشاهده در یوتیوب

## ۲۸. فرض کنید همه چیز ثبت (log) می‌شه

وقتی با این ذهنیت پیش می‌رید، آگاهانه‌تر عمل می‌کنید، می‌نویسید، و حرف می‌زنید. [این مقاله](#) رو برای اطلاعات بیشتر بخونید.

## ۲۹. نرم افزارهای ناشناخته رو نصب نکنید

حتماً صحت امضای نرم افزار رو در صورت وجود احراز و، البته، قبل از وارد کردن کلید سازنده نرم افزار از اصالت اون اطمینان حاصل کنید. به قولی، “don't trust, verify” اینجا بسیار حائز اهمیتیه. برای اطلاعات بیشتر در مورد احراز و اصالت سنجی نرم افزارها به راهنمای جامع PGP رجوع کنید.



آموزش تصویری اصالت سنجی فایل ها در یوتیوب

## ۳۰. نرم افزارهای ناشناخته رو در محیط ماشین مجازی (virtual machine) اجرا کنید

اجرای نرم افزارها در محیط ماشین مجازی امکان بروز خطر رو تا حد زیادی کاهش می ده. مفهوم sandbox و ابزارهایی مثل Sandboxie هم بسیار کارآمدن. در موردشون بخونید.

## ۳۱. قانون رو زیر پا نذارید

انجام کارهای غیرقانونی توجه افراد و سازمان ها رو به شما جلب می کنه—به همین سادگی.

## ۳۲. نسخه پشتیبان (backup) تهیه کنید؛ صحت نسخه پشتیبان رو بررسی کنید

توجه کنید که نسخه پشتیبانی که بررسی و صحت سنجی نشده، در واقع نسخه پشتیبان نیست.

### ۳۳. و به عنوان نکته‌های آخر ...

دیرباور باشید، هر چیزی رو تا زمانی که اصالتش رو احراز نکرده‌اید قبول نکنید، برنامه‌نویسی یاد بگیرید، و سؤال پرسید.  
حتماً سؤال پرسید.





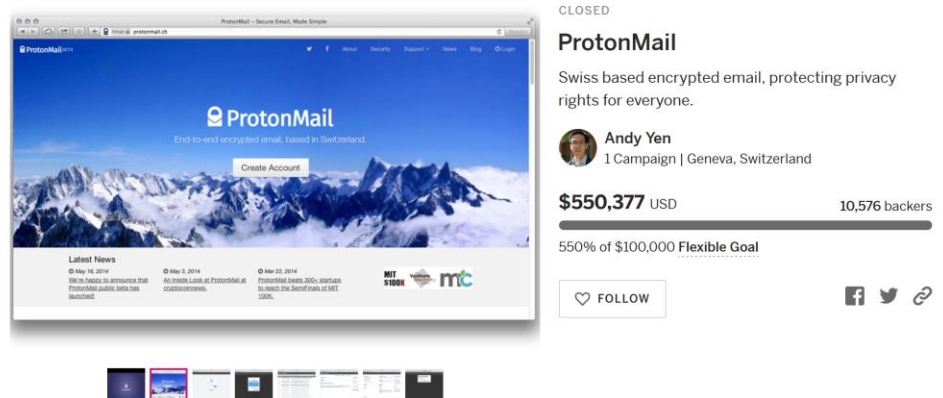
## معرفی ProtonMail: حریم خصوصی و امنیت

دهه‌ها از ظهور ایمیل می‌گذره؛ همچنان ازش استفاده می‌کنیم، و در بعضی موارد بهش وابسته‌ایم. اما خوبی دوره‌ای که در اون زندگی می‌کنیم اینه که امروز گزینه‌هامون بیشتر از سرویس‌های متداولی مثل یاهو و جی‌میلن.

در اینجا به معرفی و آموزش استفاده از سرویس پروتون‌میل خواهیم پرداخت.



شاید قبل از پرداختن به موضوع اصلی جالب باشه پیش‌زمینه کوچکی درمورد تاریخچه ایمیل پیدا کنیم. از [ریموند تاملینسون](#) به‌عنوان سازنده ایمیل و کسی که اولین پیام رو از یک کامپیوتر به کامپیوتر دیگری در شبکه ارسال کرد یاد می‌شه. این موضوع به سال ۱۹۷۱ برمی‌گرده—پنجاه سال پیش در زمان نگارش این مطلب.



کمپین جذب سرمایه جمعی پروتون میل در Indiegogo

## تاریخچه پروتون میل

در مه ۲۰۱۴، پروتون میل با هدف ارائه حریم خصوصی بیشتر به کاربرها کار خودش رو شروع کرد. استقبال به قدری زیاد بود که در انتهای ژوئیه، تنها دو ماه بعد، در کمپین جذب سرمایه جمعی شون به مبلغ باورنکردنی نیم میلیون دلار رسیدن، درحالی که هدف اولیه ۱۰۰,۰۰۰ دلار بود.

پروتون میل، که استفاده ازش در ابتدا نیازمند دریافت دعوت نامه بود، مارس ۲۰۱۶ عمومی شد، و کاربرها حالا می تونستن بدون محدودیت از این سرویس استفاده کنن. چند ماه بعد، شاهد جهشی در تعداد کاربران ایرانی بودیم، و از اون زمان تا امروز تنها می شه تصور کرد این تعداد چقدر بیشتر شده.

اما پیش از اینکه بررسی کنیم چرا پروتون میل نسبت به سرویس های دیگه بهتره (و نه راه حل نهایی)، باید در نظر داشت که ایمیل راه ارتباطی امنی نیست. روش های بسیار امن تری وجود دارن. اگه مجبورید از ایمیل استفاده کنید و به امنیت و حریم خصوصی اهمیت می دید، بهتره از ایمیل های موقت (temporary email) استفاده کنید.

## ضرورت حریم خصوصی در ارتباطات

افرادی که سعی در نقض حریم خصوصی شما دارن، از ابرشرکت‌ها گرفته تا سازمان‌های اطلاعاتی و حکومت‌ها، هیچ‌کدوم موفق به دسترسی به داده‌های شما نخواهند شد اگر از رمزنگاری سرتاسر استفاده کنید. ایالات متحده از دهه ۱۹۹۰ تا امروز در تلاش بوده شرکت‌ها رو به ساخت در پشتی (backdoor) وادار کنه. در مورد [تراشه کلپیر \(۱۹۹۳\)](#) بخونید، یا [افشاگری‌های ادوارد اسنودن در ۲۰۱۳](#).

جف شیلر از MIT در [مقاله‌ای در سال ۱۹۹۹](#) چه دقیق گفت، «ما نباید تکنولوژی نظارت رو درون استانداردها جا بی‌اندازیم. اجرای قانون قرار نبود آسون باشه. جایی که آسونه، بهش حکومت پلیسی (سرکوب‌گر) می‌گن.»



#ICYMI: During a congressional hearing this week, #FBI Director Christopher Wray discussed how end-to-end encryption threatens the FBI's mission to protect the American people from federal crimes, including crimes against children, cyberattacks, and terrorism.



مشاهده ویدئو در توئیتر

توجه داشته باشید که رمزنگاری سرتاسر بین دو کاربر پروتون‌میل به‌طور پیش‌فرض اتفاق می‌افته. وقتی برای یک کاربر جی‌میل پیامی ارسال می‌کنید، گوگل به محتوای پیام شما دسترسی داره. در نتیجه، برای امنیت و حریم خصوصی بالاتر، بهتره افرادی که باهاشون ارتباط دارید از پروتون‌میل استفاده کنن.



دفتر مرکزی Proton Technologies در ژنو، سوئیس

## تأسیس شرکت در سوئیس

یکی از برتری‌های احتمالی پروتون‌میل در تصمیم‌میشن برای تأسیس شرکت و قرارداد دادن مراکز داده‌شون در سوئیس. از نظر قانونی، سوئیس خارج از حوزه قضایی اروپا و آمریکاست، و سازمان‌های اطلاعاتی این کشورها بدون دریافت مجوزی از دادگاه سوئیس امکان دسترسی به داده‌های این شرکت رو ندارند. حتی در اون صورت، تنها چیزی که پروتون‌میل می‌تونه در اختیار اون‌ها بذاره ایمیل‌های رمزنگاری شده‌ست.

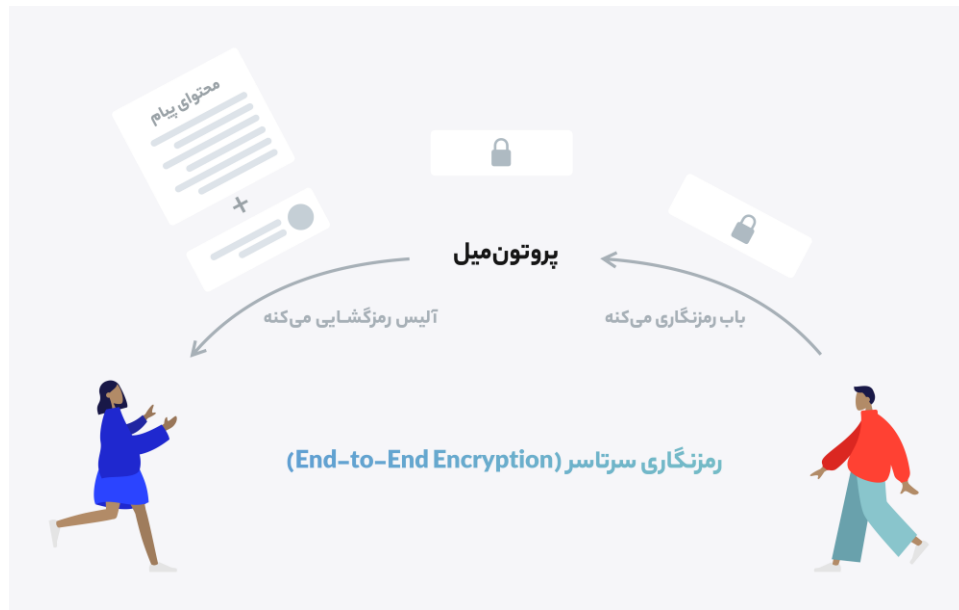
**توجه مهم:** با وجودی که پروتون‌میل ادعا می‌کنه اجباری در در اختیار قرارداد دادن داده کاربرها نداره و، حتی در صورت درخواست، داده‌ای برای ارائه نداره، در زمان نگارش این مطلب و به دستور دستگاه قضایی سوئیس آدرس آی‌پی یک فعال فرانسوی رو ثبت کرد در حالی که تا پیش از این ادعا داشت هرگز چنین کاری نمی‌کنه. بنیان‌گذار پروتون، اندی ین، در توییتی نوشته، «پروتون باید از قوانین سوئیس پیروی کنه.» به نظر میاد سوئیس تنها استثنا باشه، اما مهمه که در نظر بگیرید چرا قصد استفاده از پروتون‌میل رو دارید و آیا با مدل تهدید شما سازگار یا نه. استفاده از وی‌پی‌ان ضروریه.

50	- <b>**IP Logging:**</b> By default, we do not keep permanent IP logs in relation with your use of the Services. However, IP logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are engaged in activities that breach our terms and conditions (spamming, DDoS attacks against our infrastructure, brute force attacks, etc). The legal basis of this processing is our legitimate interest to protect our Services against nefarious activities.
50	+ <b>**IP Logging:**</b> By default, we do not keep permanent IP logs in relation with your use of the Services. However, IP logs may be kept temporarily to combat abuse and fraud, and your IP address may be retained permanently if you are engaged in activities that breach our terms and conditions (spamming, DDoS attacks against our infrastructure, brute force attacks, etc). The legal basis of this processing is our legitimate interest to protect our Services against nefarious activities. If you are breaking Swiss law, ProtonMail can be legally compelled to log your IP address as part of a Swiss criminal investigation. This obligation however does not extend to ProtonVPN ([see VPN privacy policy here](https://protonvpn.com/privacy-policy)). Additional details can be found in our [transparency report] (https://protonmail.com/blog/transparency-report).

تغییر اخیر در سیاست حریم خصوصی پروتون‌میل، که توسط [Open Terms Archive](#) گزارش شد

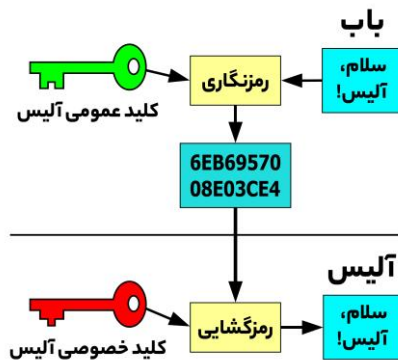
## چرا پروتون میل؟

یکی از اصلی‌ترین تفاوت‌های پروتون میل با دیگر سرویس‌ها در این است که کنترل داده شما در دست شماست. برعکس ابرشرکت‌هایی مثل گوگل و فیسبوک که مدل کسب و کارشون به دسترسی هرچه بیشتر به اطلاعات کاربرها وابسته‌ست، پروتون میل طوری طراحی شده که، حتی اگر بخواد، نمی‌تونه داده شما رو ببینه.



رمزنگاری سرتاسر در پروتون میل

وقتی از رمزنگاری سرتاسر برای ارسال پیام یا ایمیل استفاده می‌کنید، هیچ‌کسی این بین‌قادر به رمزگشایی و دیدن محتوای پیام شما نیست—نه اشخاص سوم، نه حکومت‌ها، و نه حتی پروتون میل که مکالمه شما رو ممکن کرده. این رو با امکان انقضای پیام ترکیب کنید، و دیگه عالیه.



برای درک بهتر رمزنگاری سرتاسر به مثال روبه‌رو توجه کنید. در ادامه به توضیح جزئیات اون خواهیم پرداخت. در صورتی که با مفاهیم رمزنگاری آشنا نیستید، راهنمای رمزنگاری کلید عمومی RSA شروع خوبی برای شماست. بدون شک، بعد از مطالعه‌ش، موضوع‌های مرتبط با رمزنگاری رو بهتر درک خواهید کرد.

## استفاده از رمزنگاری کلید عمومی

باب و آلیس می‌خوان خصوصی و امن با هم صحبت کنن. باب پیام خودش رو با کلید عمومی آلیس رمزنگاری می‌کنه، و در این فرآیند، «سلام، آلیس!» به متن رمزنگاری شده‌ای (ciphertext) تبدیل می‌شه، که از دید دیگران غیرقابل فهمه—EB6957008E03CE46.

باب، سپس، پیام رمزنگاری شده خودش رو ارسال می‌کنه. این پیام ممکنه از سرورهای مختلفی عبور کنه تا به مقصد برسه. در این بین، شرکت‌های واسطه ممکنه سعی کنن محتوای پیام رو بخونن، اما تبدیل متن رمزنگاری شده به متن آشکار (plaintext) بدون داشتن کلید خصوصی مرتبط غیرممکنه. درمقابل، آلیس (و تنها آلیس)، که کلید خصوصی خودش رو داره، بعد از دریافت پیام می‌تونه اون رو رمزگشایی کنه و بخونه.



وقتی آلیس می‌خواد پاسخی برای باب ارسال کنه، همین فرآیند رو تکرار می‌کنه: پیامش رو با کلید عمومی باب رمزنگاری و اون رو ارسال می‌کنه. تنها باب قادر به خوندنش خواهد بود.

برتری‌ای که رمزنگاری سرتاسر به میز میاره اینه که داده شما در مقابل نشت (leak) امنه. با فرض اینکه اشخاصی به داده‌های پروتون‌میل دست پیدا کنن، قادر به خوندن اون‌ها نخواهند بود چون کلید رمزگشایی اون‌ها دست هر کاربره. حتی پروتون‌میل هم از محتوای پیام‌های ردوبدل‌شده بی‌اطلاعه.

## ارسال ایمیل به کاربران غیر پروتون میل

شما می‌توانید ایمیل‌هایی رو هم که برای کاربرهای دیگه ارسال می‌کنید رمزنگاری کنید، با یک قدم ساده: برای پیام رمز تعیین کنید و سرنخی (hint) بذارید که فقط طرف مقابل خواهد دونست. این پیام‌ها به‌طورپیش‌فرض بعد از بیست و هشت روز منقضی می‌شن. تاریخ انقضا رو می‌تونید دستی هم وارد کنید. به تصاویر زیر توجه کنید.

The screenshot shows the 'New message' interface in ProtonMail. On the left, there's a sidebar with fields for 'From' (saeid@protonmail.com), 'Recipients', and 'Subject', along with a rich text editor. Below the editor, it says 'Sent with ProtonMail Secure Email.' At the bottom left, there's an 'Encryption' dropdown menu. On the right, a panel titled 'Encrypt for non-ProtonMail users' is open, containing three input fields: 'Message Password', 'Confirm Password', and 'Password Hint (Optional)'. A yellow warning box below these fields states: 'Encrypted messages to non-ProtonMail recipients will expire in 28 days unless a shorter expiration time is set.' At the bottom, there are 'SEND', 'CANCEL', and 'SET' buttons.

## چند نکته در باب انقضای پیام‌ها

The screenshot shows the 'Expiration time' dialog box. It has a title 'Expiration time' and a subtitle 'This message will expire in'. Below this, there are three dropdown menus for 'Weeks' (set to 4), 'Days' (set to 0), and 'Hours' (set to 0). A yellow warning box below the dropdowns says: 'If you are sending this message to a non ProtonMail user, please be sure to set a password for your message.' At the bottom, there are 'CANCEL' and 'SET' buttons.

فقط پیام‌های رمزنگاری شده امکان انقضا دارن: (۱) بین دو کاربر پروتون میل؛ (۲) رمزنگاری شده برای کاربران غیر پروتون میل. تاریخ انقضا به محض زدن گزینه ارسال شروع می‌شه، نه از زمان خوندن پیام توسط گیرنده، و بیشترین زمان انقضا چهار هفته‌ست (بیست و هشت روز).



## رمزنگاری zero-access

پروتون‌میل از روشی با عنوان رمزنگاری zero-access استفاده می‌کند. با این نوع رمزنگاری، حتی آگه داده‌ها لو یا به‌سرقت برن، قابل رمزگشایی نخواهند بود. برای درک تفاوت رمزنگاری zero-access و رمزنگاری سرتاسر به این سناریو توجه کنید.

وقتی از سرویسی غیر از پروتون‌میل—برای مثال، جی‌میل—پیامی دریافت می‌کنید، سرورهای پروتون‌میل به فاصله رسیدن ایمیل و رمزنگاری‌اش می‌تونن اون رو بخونن چون جی‌میل از رمزنگاری سرتاسر پشتیبانی نمی‌کنه. اما به محض دریافت ایمیل، پروتون‌میل اون رو با کلید عمومی کاربر رمزنگاری و سپس نگهداری می‌کنه. از اون‌پس، پروتون‌میل هرگز قادر به رمزگشایی اون پیام نخواهد بود، و تنها کسی که این امکان رو داره خود کاربره. به این روش رمزنگاری zero-access می‌گیم.

درمقابل، وقتی برای کاربر پروتون‌میل دیگه‌ای ایمیل ارسال می‌کنید، اون پیام روی دستگاه شما و با کلید عمومی گیرنده پیام رمزنگاری می‌شه، قبل از اینکه بخواد به دست پروتون‌میل برسه. در نتیجه، تنها فرستنده و گیرنده از محتوای باخبرن. این رمزنگاری سرتاسره.

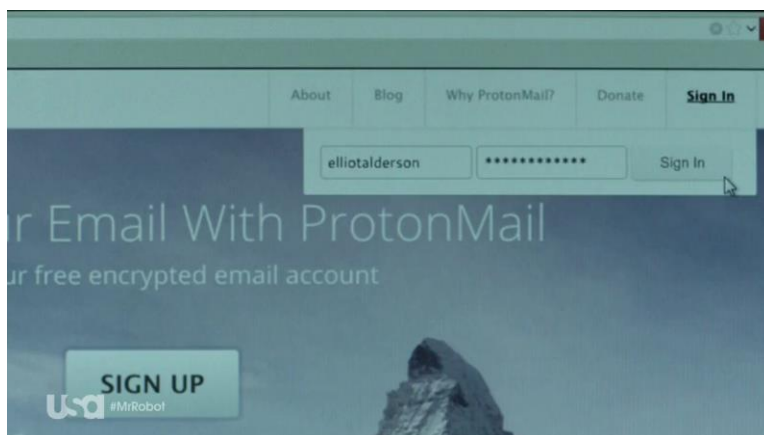
بین رمزنگاری سرتاسر و رمزنگاری zero-access، اولی قوی‌تره از این جهت که پروتون‌میل به‌هیچ‌عنوان امکان دیدن پیام رو نداره. رمزنگاری zero-access از اصل داده شما در صورت نشت یا سرقت محافظت می‌کنه، اما برای کسری از ثانیه (فاصله رسیدن پیام تا رمزنگاری) اون رو برای پروتون‌میل قابل دسترس می‌کنه. به‌همین خاطر، آگه پیامی با حساسیت بالا دارید، توصیه می‌شه دو طرف پروتون‌میل داشته باشن.

توجه کنید که پروتون‌میل یک ابزاره. فرقی نمی‌کنه که در سوئیسه. فرقی نمی‌کنه که ادعای کنه امنیت و حریم خصوصی بهتری ارائه می‌ده. درنهایت، شما، به‌عنوان کاربر، در استفاده کارآمد ازش مسئولید.



## مستر ربات

قبل از اینکه به جزئیات روش رمزنگاری پروتون‌میل بپردازم، دوست دارم گذری به سریال [مستر ربات](#) داشته باشیم. این مجموعه، که داستان شخصی به نام الیوت رو دنبال می‌کند، یکی از واقع‌گرایانه‌ترین آثاریه که می‌تونید در مورد امنیت، هک، و دنیای کامپیوتر ببینید. (این یک نظر شخصی نیست.)



صفحه ورود پروتون‌میل در سریال [مستر ربات](#) (فصل اول، قسمت هشتم)

در فصل اول [مستر ربات](#)، الیوت رو می‌بینیم که از پروتون‌میل استفاده می‌کند. این جزئیات در نگاه اول کوچک و کم‌اهمیت به نظر می‌آید، اما داستان پشتش و مکالمه‌های مفصلی که سازندگان سریال با تیم پروتون‌میل در این باره داشته‌اند نشان از توجه بالا به واقع‌گرایی و کیفیت بی‌نظیر نتیجه نهایی داره.

قسمت هشتم اوت ۲۰۱۵ به نمایش دراومد. [از قول تیم پروتون‌میل](#)، وقتی سازندگان [مستر ربات](#) در ژوئن باهاشون تماس گرفتن، از این سطح از تحقیق برای پیدا کردن سرویس ایمیل امنی که شخصیتی مثل الیوت—یک هکر و متخصص امنیت—ازش استفاده کنه تعجب کردن. به راحتی می‌تونستن این جزئیات ریز رو نادیده بگیرن. اما داستان به اینجا ختم نمی‌شه، و همکاری این دو تیم به جاهای بسیار خوبی می‌رسه. سازندگان سریال به این نکته اشاره کردن که الیوت، با توجه به شخصیت امنیت‌محوری که داره، نیازمند راهیه که بتونه فعالیت‌های ایمیلی‌اش رو نظارت کنه، و پرسیدن آیا پروتون‌میل از چنین امکانی پشتیبانی می‌کنه.

Attempt	Time	IP
LOGIN SUCCESS	2015-05-08, 22:22:07	138.203.219.111
LOGOUT	2015-05-07, 17:40:00	15.22.198.243
LOGIN SUCCESS	2015-05-07, 17:32:05	15.22.198.243
LOGIN FAILED	2015-05-07, 17:32:01	15.22.198.243
LOGOUT	2015-05-07, 17:31:52	15.22.198.243
LOGOUT	2015-05-06, 18:06:10	122.241.186.238
LOGIN SUCCESS	2015-05-06, 17:58:08	122.241.186.238
LOGOUT	2015-05-03, 02:55:52	183.100.43.197
LOGIN SUCCESS	2015-05-03, 02:31:03	183.100.43.197
LOGOUT	2015-05-02, 18:10:40	246.104.157.9
LOGIN SUCCESS	2015-05-02, 17:42:21	246.104.157.9
LOGIN FAILED	2015-05-02, 17:42:18	246.104.157.9
LOGOUT	2015-04-22, 14:59:55	15.225.10.177
LOGIN SUCCESS	2015-04-22, 23:53:45	15.225.10.177
LOGIN FAILED	2015-04-21, 12:00:53	15.225.10.177

گزارش دسترسی حساب، که به پیشنهاد سازندگان سریال اضافه شد

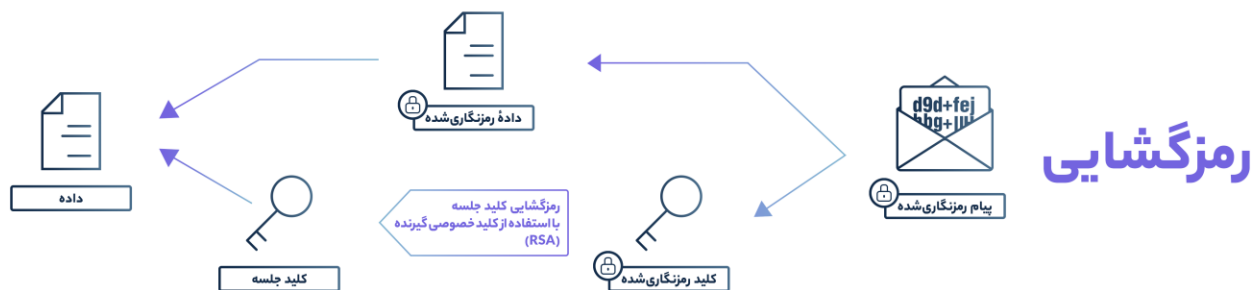
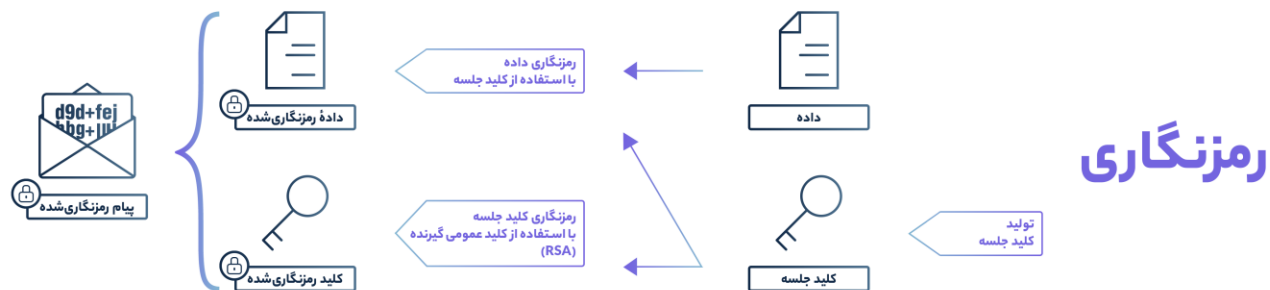
و به این شکل، این امکان به پروتون میل اضافه شد. به لطف پیشنهاد بسیار خوب سازندگان مستر ربات، شما هم می‌تونید گزارش جامعی از فعالیت‌های حسابتون رو ببینید. اینجاست که می‌بینیم سطح توجه و تحقیق این تیم، چه در کار خودشون و چه در پروتون میل، چقدر تأثیرگذار بوده. ایوت دو سال بعد و در فصل سوم همچنان از پروتون میل استفاده می‌کنه، و جالبه که هر دو بار در قسمت هشتم فصل اتفاق افتاده.

فکر می‌کنم آماده‌ایم تا به جزئیات رمزنگاری بپردازیم.

## بهره‌مندی از PGP

به‌طور خلاصه، پروتون میل از رمزنگاری PGP استفاده می‌کنه. در صورت عدم آشنایی با مفاهیم رمزنگاری، درک این بخش سخت خواهد بود. پیشنهاد می‌کنم ابتدا مطالب رمزنگاری کلید عمومی RSA و راهنمای جامع PGP رو از اینجا مطالعه کنید و سپس به این بخش برگردید.

پروتون میل از ترکیبی از رمزنگاری متقارن و نامتقارن برای ارائه رمزنگاری سرتاسر بهره می‌بره. وقتی کاربر حساب پروتون میل می‌سازه، مرورگرش یک جفت کلید RSA تولید و از کلید عمومی برای رمزنگاری ایمیل‌ها و سایر داده‌های کاربر استفاده می‌کنه. کلید خصوصی با گذرواژه حساب رمزنگاری می‌شه.



اولین کاری که PGP انجام می‌ده تولید یک کلید جلسه (session key) طولانیه. از این کلید برای رمزنگاری محتوای پیام (داده) استفاده می‌شه. کلید جلسه—که منحصر به فرد و با هر پیام تغییر می‌کنه—سپس با کلید عمومی گیرنده رمزنگاری می‌شه.

به زبان ساده‌تر، پیام رو با استفاده از رمزنگاری متقارن و به کمک کلید جلسه رمز و به متنی غیرقابل فهم تبدیل می‌کنیم. حالا یک داده رمزنگاری شده و یک کلید آشکار داریم. سپس، کلید جلسه رو با استفاده از رمزنگاری نامتقارن، با کلید عمومی گیرنده، رمز و برای او ارسال می‌کنیم. به شکل بالا توجه کنید.

گیرنده پیام، که کلید خصوصی خودش رو داره، ابتدا کلید جلسه رو رمزگشایی و با کمک اون محتوای پیام رو باز می‌کنه—سریع، امن، و بدون دردسر.

چرا قدم اضافی؟ چرا داده رو مستقیم با کلید عمومی گیرنده رمزنگاری نکنیم؟ سؤال بسیار خوبییه.

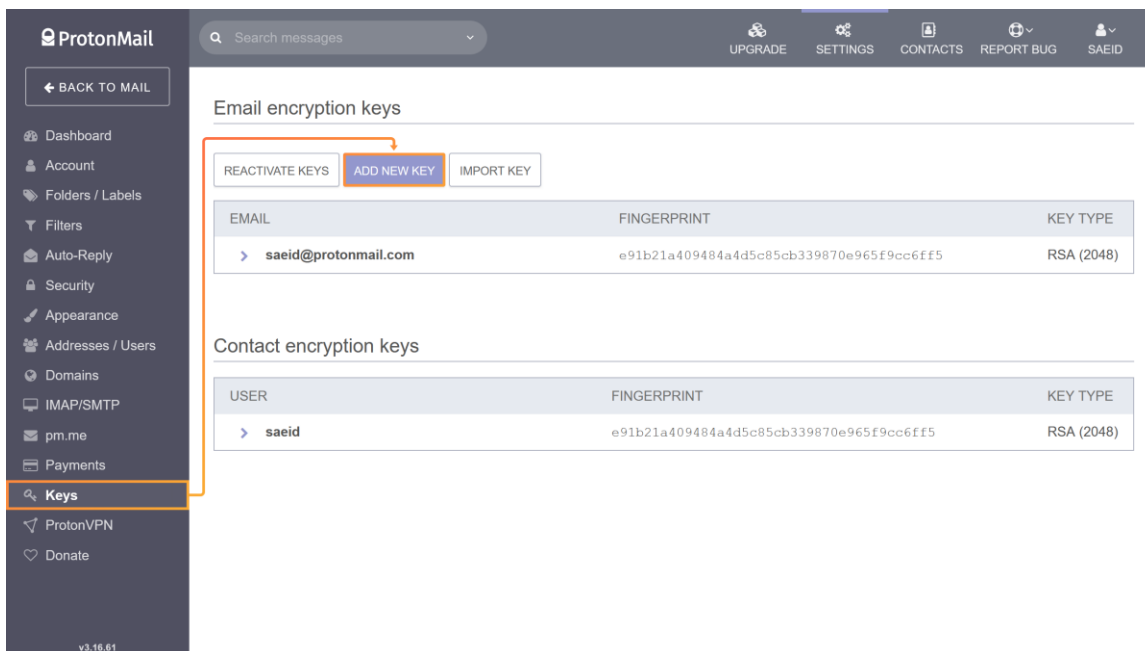
رمزنگاری کلید عمومی به‌طورکلی روش کندی محسوب می‌شود—بسیار کندتر از روش‌های متقارن. هرچقدر پیام و ضمیمه بلندتر و بزرگ‌تر باشد، رمزنگاری یا رمزگشایی اون‌ها زمان و قدرت پردازشی بیشتری می‌طلبد. روش فعلی سرعت و بهینگی رمزنگاری متقارن رو همراه با امنیت رمزنگاری کلید عمومی به ما می‌دهد.

این روش دو جنبهٔ دیگه هم داره، که قابل توجهه. در PGP با مفهوم امضای دیجیتال آشنا شده‌ایم. امضای دیجیتال این اطمینان رو به گیرنده می‌ده که پیامی که دریافت کرده حتماً از سمت فرستنده اومده. هر تغییری در پیام (یا کلید خصوصی امضاکننده) امضا رو نامعتبر می‌کنه.

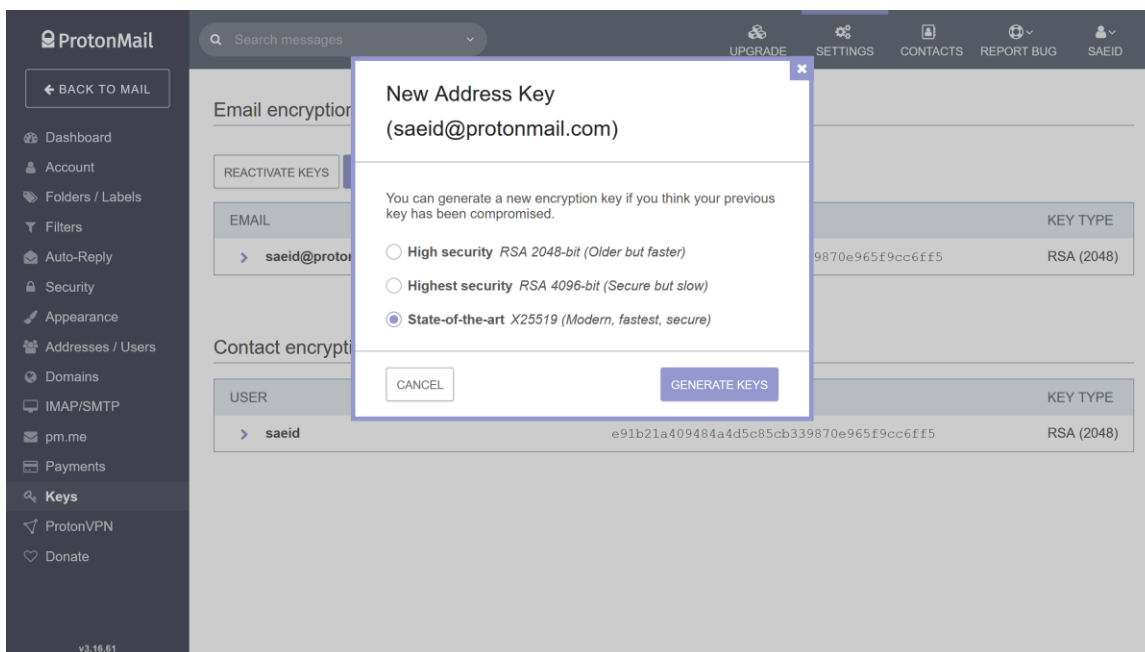
از طرفی، فرستنده چطور می‌تونه اعتماد کنه که کلید عمومی‌ای که برای رمزنگاری پیام و ارسالش به گیرنده استفاده می‌کنه به همون شخص تعلق داره؟ سرور می‌تونه یک کلید عمومی قلابی در اختیار فرستنده قرار بده. برای حل این مشکل، پروتون‌میل احراز آدرس ([Address Verification](#)) رو معرفی کرده. شما می‌تونید کلیدهای مخاطبین خودتون رو در پروتون‌میل به‌صورت دیجیتالی امضا—و اون‌ها کلید شما رو—و به این شکل به اون‌ها اعتماد کنید. در حال حاضر، پروتون‌میل در حال کار روی امکانی با عنوان Key Transparency است، که کلید عمومی گیرنده‌ها رو خودکار احراز می‌کنه.

## تغییر نوع کلید

در نظر داشته باشید که وقتی حساب می‌سازید، پروتون‌میل به‌صورت پیش‌فرض رمزنگاری RSA با کلید ۲۰۴۸ بیتی رو برای شما در نظر می‌گیره. شما می‌تونید کلید ۴۰۹۶ بیتی بسازید، یا از رمزنگاری منحنی بیضوی (ECC) برای سرعت بالاتری که ارائه می‌ده استفاده کنید. به تصاویر صفحات بعد توجه کنید.



قدم اول جهت افزودن کلید جدید با رمزنگاری منحی بیضوی: Keys → Add New Key



قدم دوم: State-of-the-art → Generate Keys

The screenshot shows the ProtonMail interface. On the left is a sidebar with navigation options like Dashboard, Account, Folders / Labels, Filters, Auto-Reply, Security, Appearance, Addresses / Users, Domains, IMAP/SMTP, pm.me, Payments, Keys, ProtonVPN, and Donate. The main content area is titled 'Email encryption keys' and contains buttons for 'REACTIVATE KEYS', 'ADD NEW KEY', and 'IMPORT KEY'. Below these are two tables. The first table lists email keys for 'saeid@protonmail.com' with columns for EMAIL, FINGERPRINT, and KEY TYPE. The second table provides a detailed view of the keys with columns for FINGERPRINT, KEY TYPE, STATUS, and ACTIONS. The 'Contact encryption keys' section below it shows a table with columns for USER, FINGERPRINT, and KEY TYPE, listing the user 'saeid'.

قدم سوم: انتخاب فلش کنار Export برای کلید تازه تولید شده

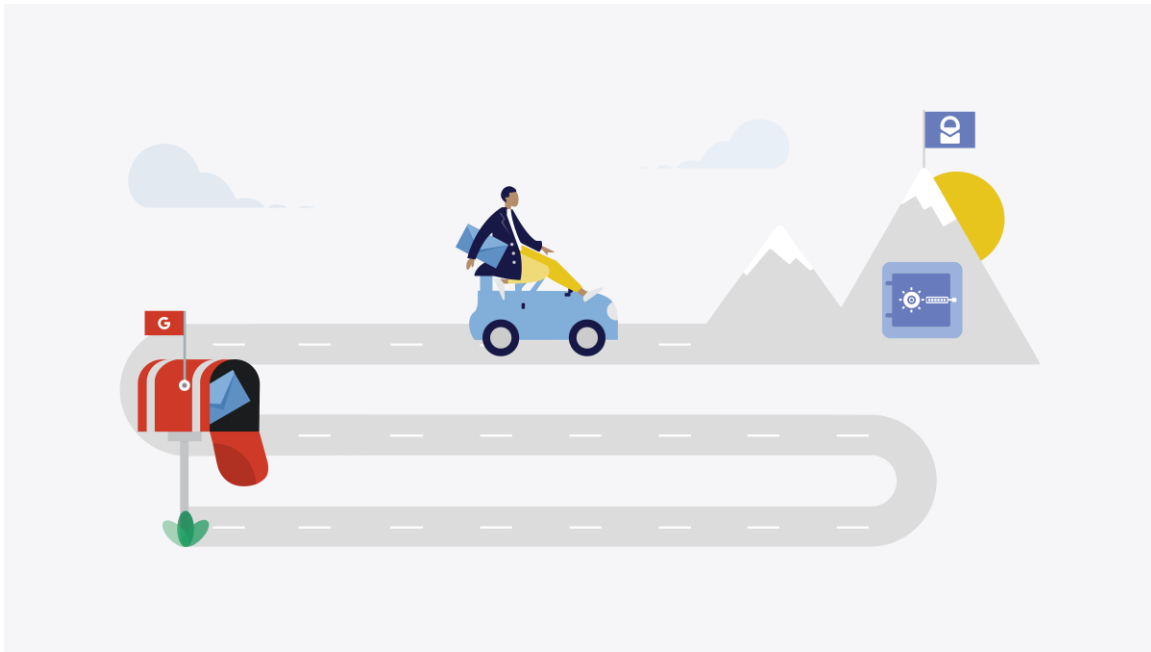
This screenshot is similar to the first one but shows a context menu open over the 'EXPORT' button in the 'Email encryption keys' table. The context menu options are 'MAKE PRIMARY', 'MARK OBSOLETE', 'MARK COMPROMISED', and 'DELETE'. The 'Email encryption keys' table and 'Contact encryption keys' table are also visible.

قدم چهارم و آخر: انتخاب گزینه Make Primary جهت استفاده از کلید تازه تولید شده به عنوان کلید اصلی

برای مطالعه جزئیات فنی رمزنگاری منحنی بیضوی به این مقاله رجوع کنید.

## مهاجرت از سرویس های دیگه به پروتون میل

شما همچنین می تونید از سرویس های دیگه، مثل جی میل یا یاهو، به پروتون میل مهاجرت کنید، و نه تنها تمام ایمیل ها و فایل هاتون رو داشته باشید بلکه ایمیل های دریافتی در اون سرویس ها هم مستقیم به آدرس جدیدتون در پروتون میل فرستاده بشن. در این بخش به چگونگی این کار خواهیم پرداخت.



تصویر مقاله [How to migrate from Gmail to ProtonMail](#): بازطراحی شده توسط امیر آریا

برای انجام این کار در جی میل، ابتدا وارد تنظیمات جی میل شده و اطمینان حاصل کنید IMAP در بخش Forwarding فعاله. به Labels رفته و انتخاب کنید چه پوشه هایی رو می خواید انتقال بدید. به تصاویر صفحات بعد توجه کنید.

**Settings**

General Labels **Inbox** Accounts and Import Filters and Blocked Addresses

Forwarding and POP/IMAP Add-ons Chat and Meet Advanced Offline Themes

**Forwarding:** [Learn more](#) **Add a forwarding address**

Tip: You can also forward only some of your mail by [creating a filter!](#)

**POP download:** [Learn more](#)

- Status: POP is enabled** for all mail that has arrived since 12/23/11
  - Enable POP for **all mail** (even mail that's already been downloaded)
  - Enable POP for **mail that arrives from now on**
  - Disable POP**
- When messages are accessed with POP**  
keep Gmail's copy in the Inbox
- Configure your email client** (e.g. Outlook, Eudora, Netscape Mail)  
[Configuration instructions](#)

**IMAP access:** (access Gmail from other clients using) **Status: IMAP is enabled**

- Enable IMAP
- Disable IMAP

قدم اول: اطمینان از فعال بودن IMAP در بخش Forwarding

**Settings**

General **Labels** Inbox Accounts and Import Filters and Blocked Addresses

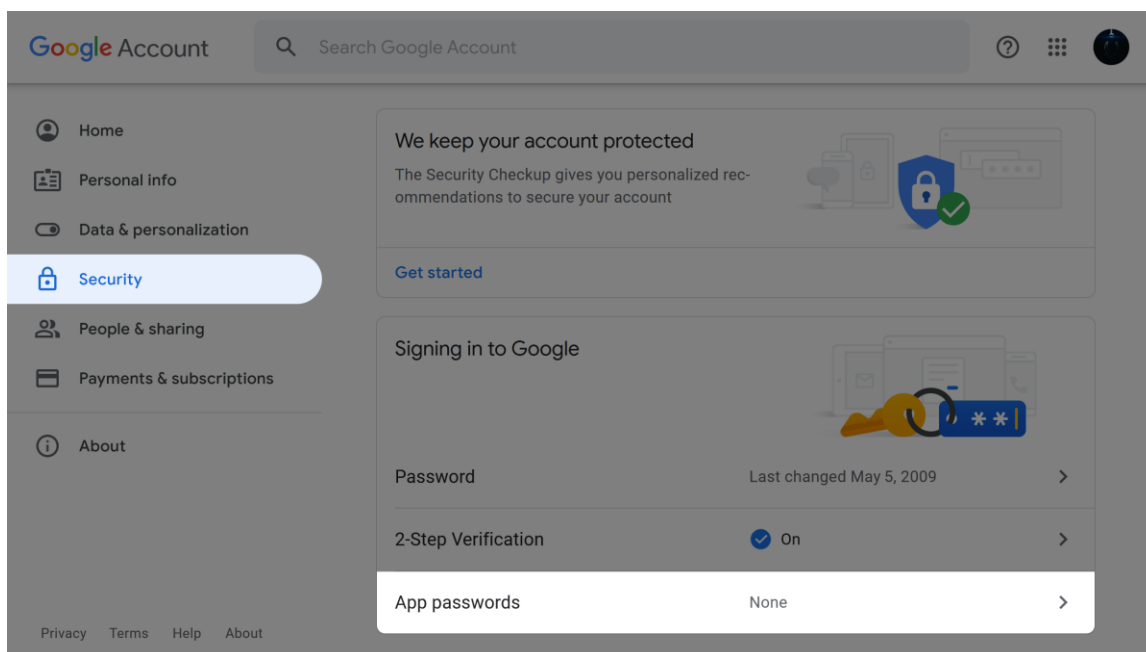
Forwarding and POP/IMAP Add-ons Chat and Meet Advanced Offline Themes

System labels	Show in label list	Show in IMAP
Inbox		<input checked="" type="checkbox"/> Show in IMAP
Starred	<a href="#">show</a> <a href="#">hide</a>	<input checked="" type="checkbox"/> Show in IMAP
Snoozed	<a href="#">show</a> <a href="#">hide</a>	<input checked="" type="checkbox"/> Show in IMAP
Important	<a href="#">show</a> <a href="#">hide</a>	<input checked="" type="checkbox"/> Show in IMAP
Chats	<a href="#">show</a> <a href="#">hide</a>	<input type="checkbox"/> Show in IMAP
Sent	<a href="#">show</a> <a href="#">hide</a>	<input checked="" type="checkbox"/> Show in IMAP
Scheduled	<a href="#">show</a> <a href="#">hide</a> <a href="#">show if unread</a>	<input checked="" type="checkbox"/> Show in IMAP
Drafts	<a href="#">show</a> <a href="#">hide</a> <a href="#">show if unread</a>	<input checked="" type="checkbox"/> Show in IMAP
All Mail	<a href="#">show</a> <a href="#">hide</a>	<input checked="" type="checkbox"/> Show in IMAP

قدم دوم: انتخاب پوشه‌های موردنظر در Labels



حالا به تنظیمات حساب گوگل برید، در Security وارد App passwords بشید، و رمزی برای پروتون میل بسازید.



Google Account

## ← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

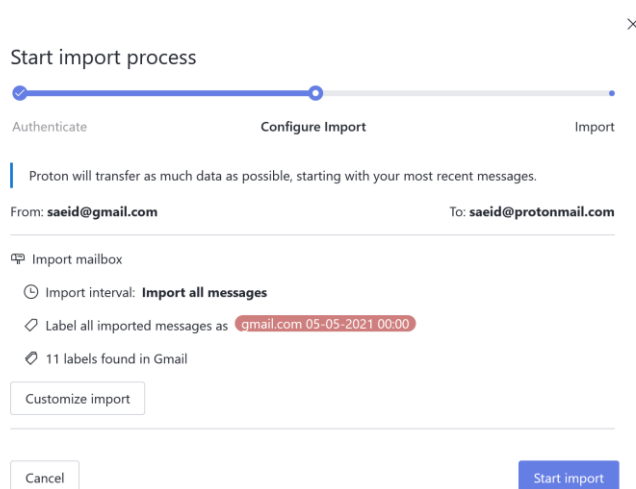
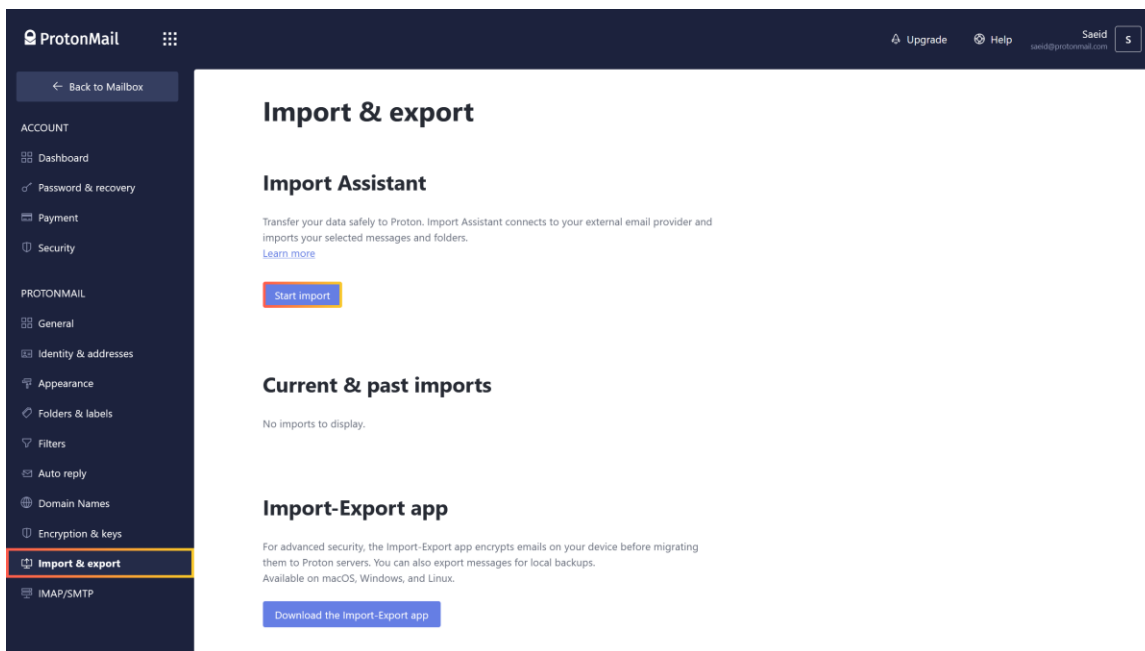
Select the app and device you want to generate the app password for.

Select app	Select device	
Mail		GENERATE
Calendar		
Contacts		
YouTube		
Other (Custom name)		

Privacy Terms Help About

Security → App passwords در تعیین رمز برای پروتون میل

اگه App passwords رو نمی بینید، به این دلیل که احراز دو عاملی (two-factor authentication) رو فعال نکردید، که در این حالت، توصیه می کنم اولین کاری که انجام می دید فعال کردنش باشه. در صورتی که احراز دو عاملی فعال نباشه، به جای App passwords گزینه Turn on access رو خواهید دید.



در انتها، وارد سایت پروتون میل بشید، وارد حساب بشید، در تنظیمات به بخش Import Assistant برید (که در نسخه بتا Import & export نام داشت)، و Start import رو بزیند. آدرس جی میل رو همراه با رمزی که در App Passwords گرفتید وارد کنید، و پروتون میل بقیه کارها رو برای شما انجام می ده. یا هو هم روند مشابهی داره، اما اگه سؤالی بود، پیرسید.

قدم چهارم و آخر: Import Assistant → Start import

درضمن، شما می تونید از آدرس های کوتاه شده @pm.me هم استفاده کنید (به عبارتی، PM me یا بهم پیام خصوصی بده). هر بار نوشتن protonmail.com می تونه سخت باشه، چه برای شما و چه شخص مقابل. برای این کار، به تنظیمات و بخش pm.me برید. کاربرهای مجانی فقط می تونن به این آدرس ها دریافت کنن.

بسیار عالی. با کلیات پروتون میل آشنا شدیم.

## سخن پایانی

بالا تر به امنیت پایین ایمیل و ضرورت استفاده از آدرس‌های موقت اشاره کردیم. ابزار [Firefox Relay](#) رو برای این کار در نظر داشته باشید. همچنین، از یک ایمیل برای همهٔ ثبت‌نام‌ها استفاده نکنید.

برای ساختن حساب نیاز به وارد کردن شمارهٔ تلفن ندارید، اما آگه سرویسی از شما درخواست کرد، توجه داشته باشید که این موضوع حریم خصوصی شما رو تحت تأثیر قرار می‌ده. در صورت نیاز از شماره‌های مجازی استفاده کنید.

آگه بخوام یک منبع معرفی کنم که اطلاعاتتون رو کامل کنه، ویدئوی ارائهٔ [بارت باتلر](#) مدیر ارشد تکنولوژی پروتون میله، که می‌تونید اون در [Vimeo](#) ببینید. در دقیقهٔ دوازده، جایی که داره در مورد تجربهٔ کاربری (UX) صحبت می‌کنه، نقل قول جالبی از بروس اشنایر (Bruce Schnier) میاره.

در نهایت، مهم‌ترین اصل اینه: [DYOR](#) (خودت تحقیق کن). پروتون میل بهترین نیست، اما گزینهٔ خوبیه. [اشکال‌هایی](#) بهش [وارد](#)، و خوبه که بدونیم اون‌ها چی‌ان. بدون شک پیشرفت‌های زیادی داشته، اما بی نقص نیست. در نتیجه، تنها به حرف من اتکا نکنید، به خصوص وقتی پای امنیت و حریم خصوصی درمیونه.



## حریم خصوصی در فایرفاکس

وقتی صحبت از حریم خصوصی می‌شه، مرورگر **فایرفاکس** یک سرگردن 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](https://privacytools.io/#browser-addons)

## بررسی وضعیت اثرانگشت مرورگر

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

The screenshot shows the EFF Cover Your Tracks interface. On the left, a green sidebar contains the EFF logo, the title 'COVER YOUR TRACKS', a link 'See how trackers view your browser', the heading 'TESTING YOUR BROWSER', and a brief description of the project. The main content area on the right displays the 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, a table titled 'IS YOUR BROWSER:' shows the following results:

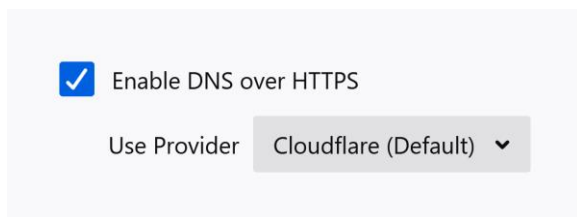
Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

ابزار سنجش وضعیت اثرانگشت سایت EFF

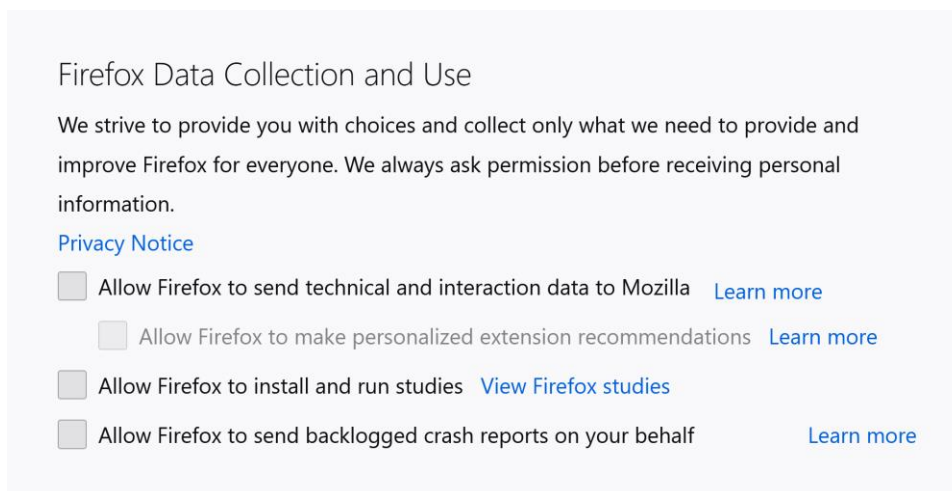
پیشنهاد من اینه که درمورد اثرانگشت آگاه باشید، اما دغدغه اصلی شما نباشه. درعوض، سعی کنید با استفاده از افزونه‌های مناسب کنترل جریان اطلاعات و حریم خصوصی خودتون رو به دست بگیرید.

## 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.



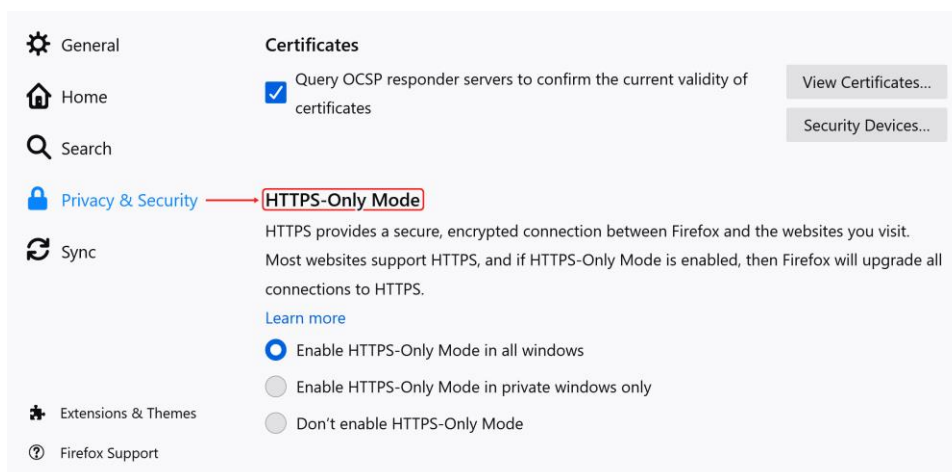
Firefox Data Collection and Use

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

Home

Search

Privacy & Security **HTTPS-Only Mode**

Sync

Extensions & Themes

Firefox Support

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

[Security Devices...](#)

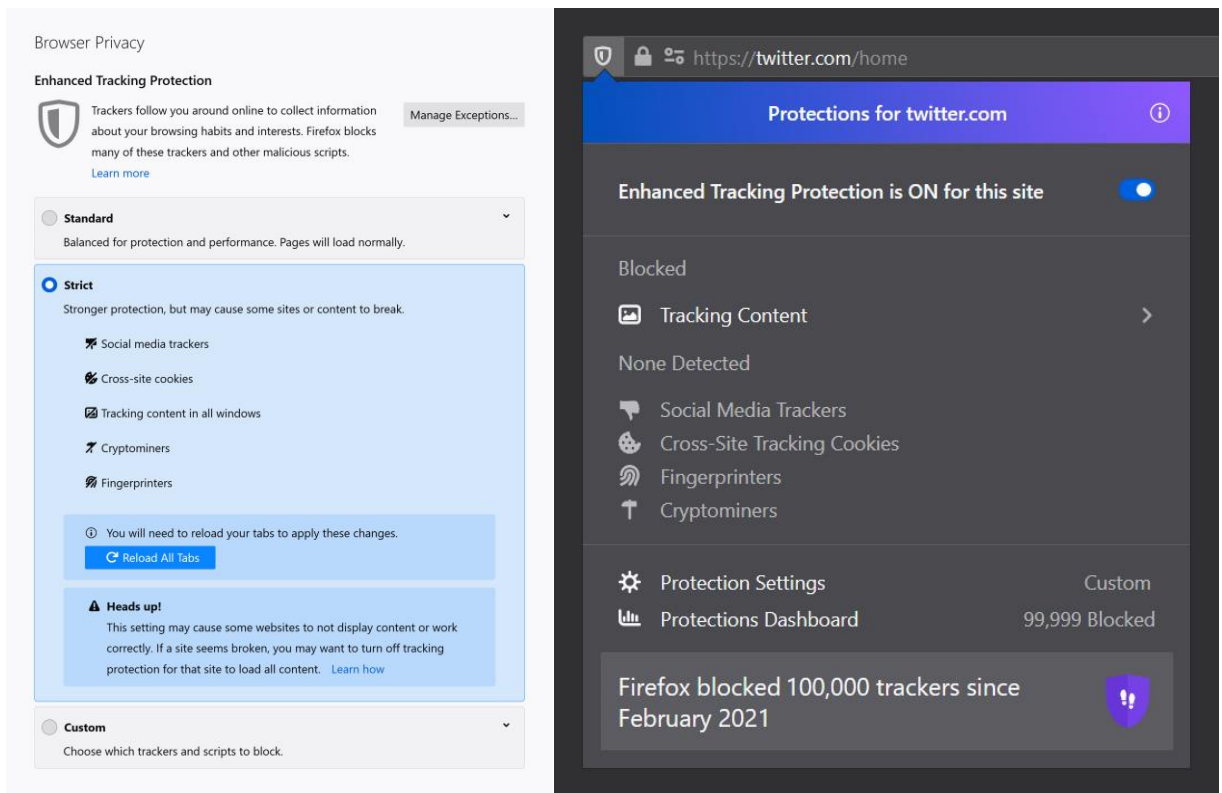
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

[Learn more](#)

- Enable HTTPS-Only Mode in all windows
- Enable HTTPS-Only Mode in private windows only
- Don't enable HTTPS-Only Mode

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

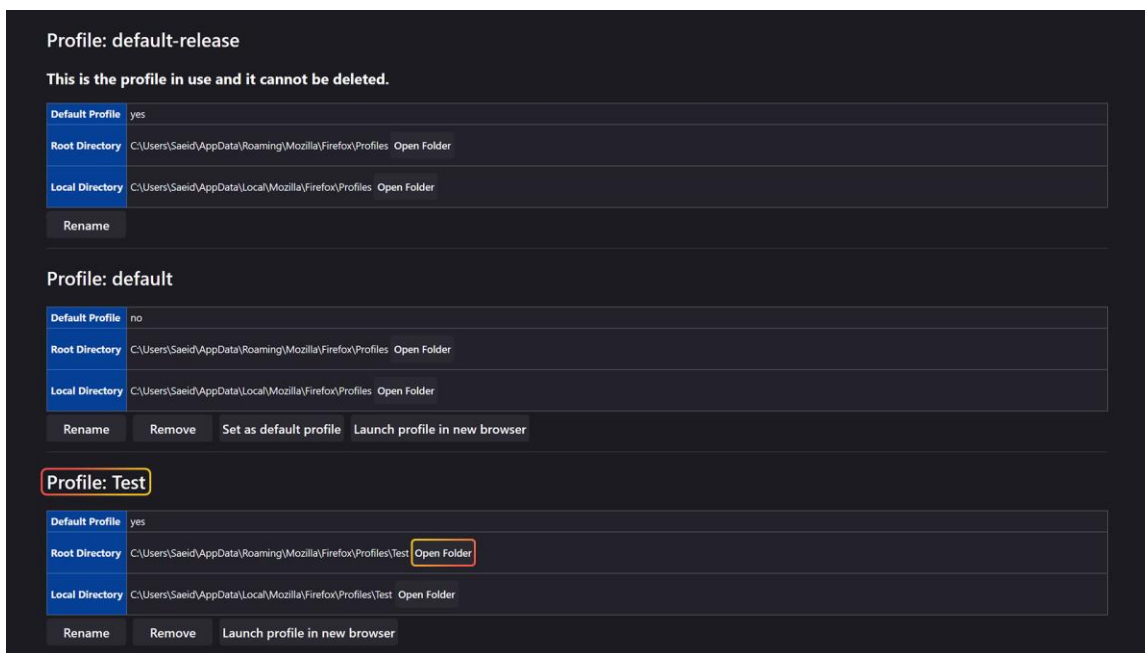
گزینه Strict بیشترین حریم خصوصی رو ارائه می‌ده، اما ممکنه باعث بشه بعضی سایت‌ها از کار بی‌افتن. بررسی کنید و ببینید چه چیزی برای شما بهتره، و اگه نمی‌دونستید، حتماً پیرسید. درضمن، حتی اگه از حالت Strict استفاده کنید، می‌تونید اون رو برای سایت‌های خاصی غیرفعال کنید.

## 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](https://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

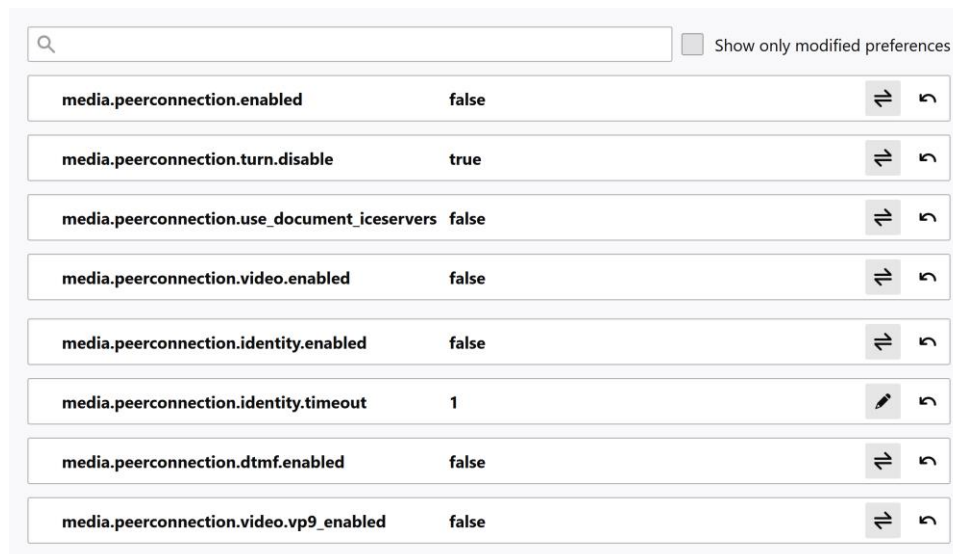
در مرحله بعد، در نوار آدرس بنویسید `about:profile` و `enter` بزنید. با انتخاب گزینه `Create a New Profile` یک پروفایل جدید ایجاد کرده و پوشه `Root Directory` مربوط به اون رو باز کنید، مثل تصویر بالا. سپس، مرورگر رو ببندید. فایل‌های موجود در پوشه **پروفایل جدید** رو پاک کرده و محتوای `profile.zip` رو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



## راه حل تخصصی

یکی از نشت‌های مهم WebRTC است. در موردش جستجو کنید و بخونید. اینجا می‌خوایم به‌طور کامل غیرفعالش کنیم.

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



The screenshot shows the `about:config` page with a search bar at the top. A checkbox labeled "Show only modified preferences" is present. Below the search bar, a list of settings is displayed, each with a name, a value, and a control icon (a double-headed arrow or a pencil). The settings are:

Setting Name	Value	Control Icon
<code>media.peerconnection.enabled</code>	false	↕
<code>media.peerconnection.turn.disable</code>	true	↕
<code>media.peerconnection.use_document_iceservers</code>	false	↕
<code>media.peerconnection.video.enabled</code>	false	↕
<code>media.peerconnection.identity.enabled</code>	false	↕
<code>media.peerconnection.identity.timeout</code>	1	✎
<code>media.peerconnection.dtmf.enabled</code>	false	↕
<code>media.peerconnection.video.vp9_enabled</code>	false	↕

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 می‌کنیم، [این مطلب](#) رو بخونید.



## ابزارهای کارآمد فایرفاکس

فایرفاکس ابزارهای قدرتمندی دارد، بعضی‌هاشون منحصر به فرد و مختص همین مرورگرن. 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](https://monitor.firefox.com)

**آدرس‌های ره خود را مدیریت کنید**



**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 به‌کلی حذف کنید.

**% تخفیف**



**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.



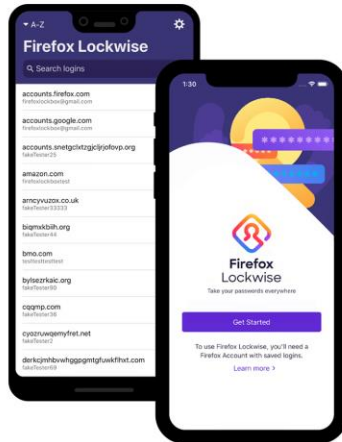
**افزونه را نصب کنید**

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.

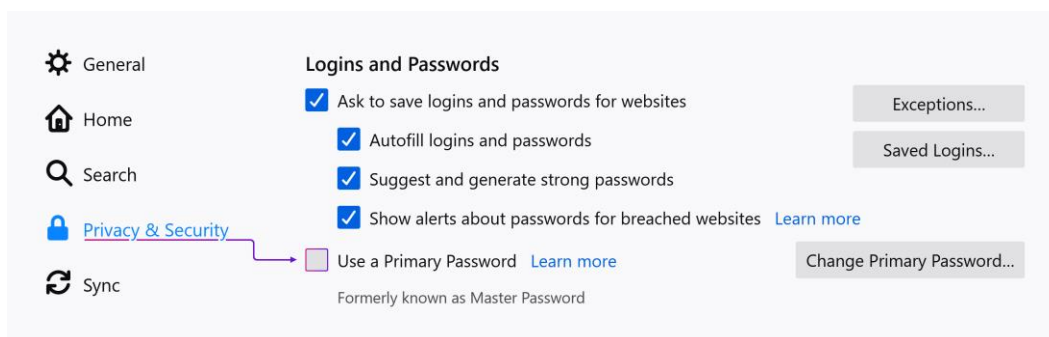
امتحانش کنید: [relay.firefox.com](https://relay.firefox.com)



## 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. در نظر 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 میان بر Ctrl + Shift + S استفاده کنید.

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.

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

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.

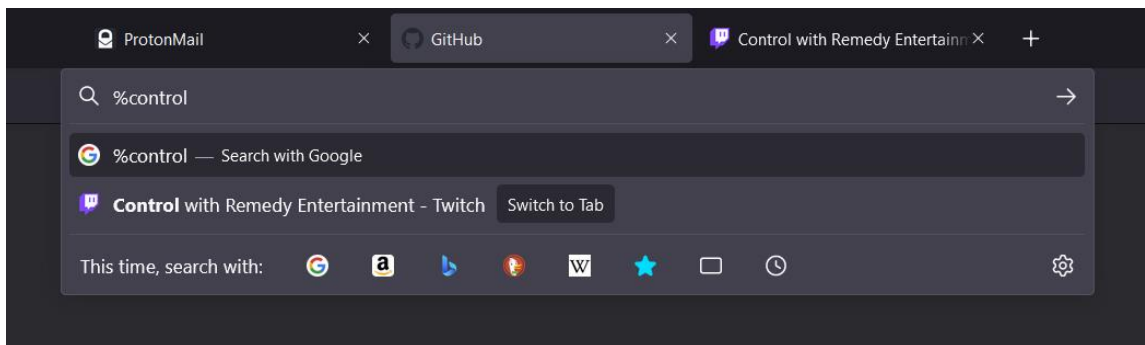
امتحانش کنید: [color.firefox.com](https://color.firefox.com)



## 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

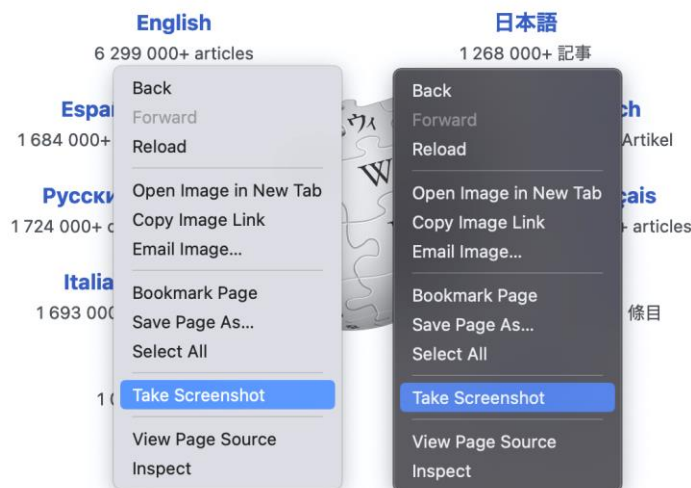


اگر شما هم مثل من کلی تب باز می‌کنید و بعد پیدا کردن یک تب خاص مثل پیدا کردن یک سوزن در انبار گاه می‌شه، کافیه در نوار آدرس یک علامت درصد (%) بذارید. حالا می‌تونید بین تب‌های باز فایرفاکس (حتی در پنجره‌های مختلف) جستجو کنید.

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



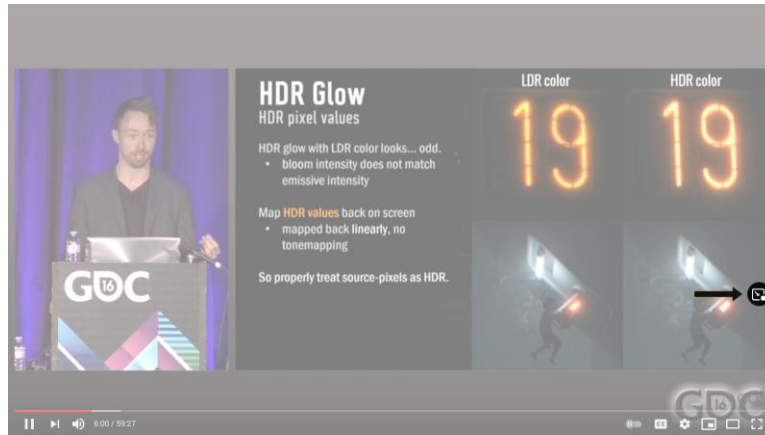
بالتر به قابلیت پیشرفته اسکرین‌شات این مرورگر پرداختیم. در هر صفحه‌ای که باشید، کافیه راست کلیک کرده و گزینه Take Screenshot رو انتخاب کنید یا، اگه مثل من بیشتر اوقات دستتون روی صفحه کلیده، کلیدهای میان‌بر **Ctrl + Shift + S** رو فشار بدید.

## بازیابی یک تب بسته‌شده

حتماً پیش اومده که تپی رو به اشتباه ببینید. چطور می‌تونید تب‌های بسته‌شده 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.

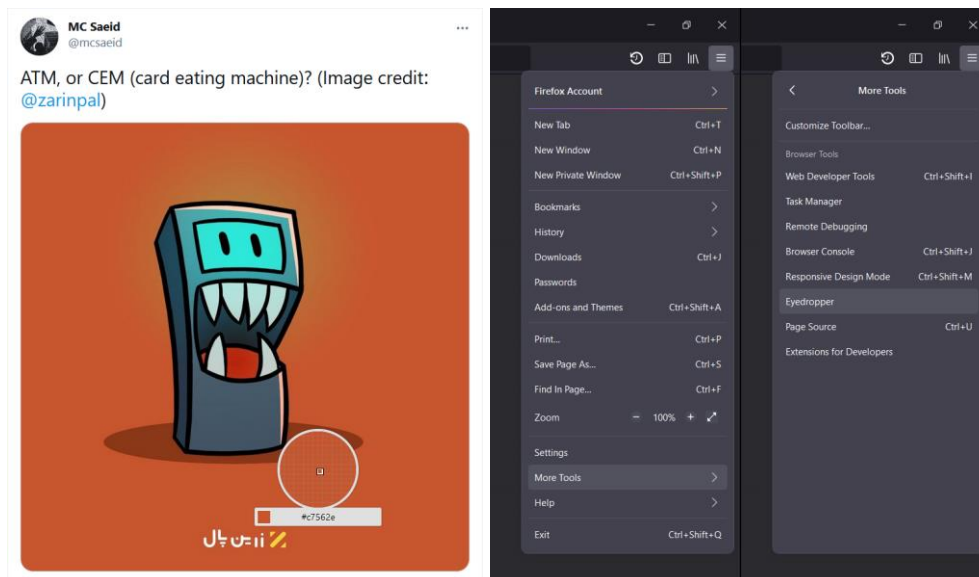
## انجام هم‌زمان چند کار



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

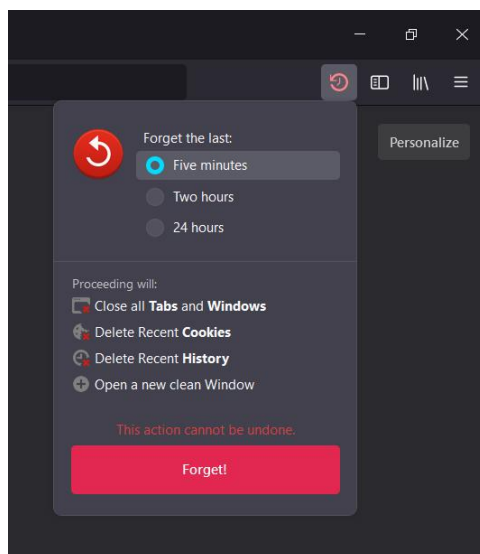
دنیای وب پر از رنگ‌های مختلف و زیبا، و هر رنگی یک کد هگزادسیمال منحصر به فرد داره. قابلیت Eyedropper، برای اون دسته که اهل طراحی‌ان، می‌تونه بسیار کاربردی باشه. از منوی اصلی سمت راست More Tools → Eyedropper رو انتخاب کنید.





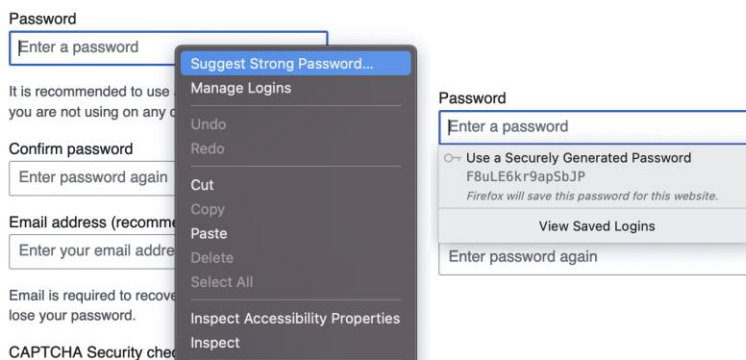
## پاک کردن سریع تاریخچه یا، به قولی، fuggedaboutit!

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.

این راهنما توسط **ام‌سی سعید** گردآوری شده است. برای دریافت مطالب آموزشی مرتبط با بیت کوین و حریم خصوصی می‌توانید به کانال تلگرام او به آدرس [t.me/dieascm](https://t.me/dieascm) مراجعه کنید.

این راهنما تحت مجوز «مالکیت عمومی» منتشر می‌شود و بازنشر آن به هر شکل آزاد است.



## bitcoind.me

### منابع فارسی بیت کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقه‌مندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند