



معرفی پروتون میل: 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 پروتون میل 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.

INDIEGOGO



CLOSED

ProtonMail

Swiss based encrypted email, protecting privacy rights for everyone.



Andy Yen

1 Campaign | Geneva, Switzerland

\$550,377 USD

10,576 backers

550% of \$100,000 Flexible Goal

FOLLOW



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 دارند، از ابرشرکت‌ها گرفته تا سازمان‌های اطلاعاتی و حکومت‌ها، هیچ‌کدام 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 کند. درمورد [تراشه کلیر \(۱۹۹۳\)](#) 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) می‌کن.»



#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 دارد. در نتیجه، برای امنیت و حریم خصوصی بالاتر، بهره‌افزایی که باهاشون ارتباط دارید از پروتون‌میل استفاده کنند.



دفتر مرکزی پروتون‌میل در ژنو، سوئیس

تأسیس شرکت در سوئیس

یکی از برتری‌های احتمالی پروتون‌میل در تصمیم‌شون برای تأسیس شرکت و قراردادن 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 ندارن. حتی دراون‌صورت، تنها چیزی که پروتون‌میل می‌تونه دراختیار اون‌ها بذاره ایمیل‌های رمزنگاری‌شده‌ست.

توجه مهم: باوجودی که پروتون‌میل ادعا می‌کنه اجباری در دراختیارقراردادن داده کاربرها نداره و، حتی درصورت درخواست، داده‌ای برای ارائه نداره، در زمان نگارش این مطلب و به دستور دستگاه قضایی سوئیس آدرس آی‌پی یک فعال فرانسوی رو ثبت کرد درحالی که تا پیش از این ادعا داشت هرگز چنین کاری نمی‌کنه. بنیان‌گذار پروتون، اندی‌ین، در توییته نوشته، «پروتون باید از قوانین سوئیس پیروی کنه.» به‌نظر میاد سوئیس تنها استثنا باشه، اما مهمه که درنظر بگیرید چرا قصد استفاده از پروتون‌میل رو دارید و آیا با مدل تهدید شما سازگاره یا نه. استفاده از وی‌پی‌ان ضروریه.

50	- **IP Logging:** 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	+ **IP Logging:** 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

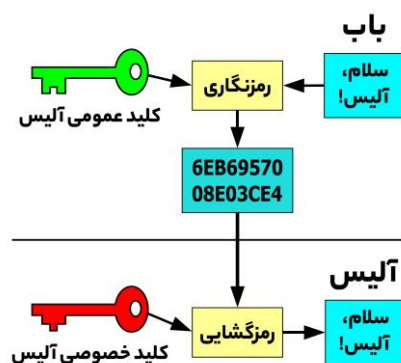
چرا پروتون میل؟

یکی از اصلی‌ترین تفاوت‌های پروتون میل با دیگر سرویس‌ها در اینه 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 اگه 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' window in ProtonMail. On the left, the 'From' field is set to 'saeid@protonmail.com'. Below it, there are fields for 'Recipients' and 'Subject'. A rich text editor toolbar is visible. The main content area says 'Sent with [ProtonMail](#) Secure Email.' At the bottom, there's an 'Encryption' button. On the right, a panel titled 'Encrypt for non-ProtonMail users' contains three input fields: 'Message Password', 'Confirm Password', and 'Password Hint (Optional)'. A yellow warning box states: 'Encrypted messages to non-ProtonMail recipients will expire in 28 days unless a shorter expiration time is set.' At the bottom of the right panel are 'CANCEL' and 'SET' buttons.

چند نکته در باب انقضای پیام‌ها

The screenshot shows the 'New message' window with the 'Expiration time' panel open. It displays 'This message will expire in' followed by three dropdown menus: '4' for Weeks, '0' for Days, and '0' for Hours. A yellow warning box 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 are 'CANCEL' and 'SET' buttons.

فقط پیام‌های رمزنگاری‌شده امکان انقضا دارن: (۱) بین دو کاربر پروتون‌میل؛ (۲) رمزنگاری‌شده برای کاربران غیر پروتون‌میل. 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

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

وقتی از سرویسی غیر از پروتون میل — برای مثال، جی میل — پیامی دریافت می‌کنید، سرورهای پروتون میل به فاصله رسیدن ایمیل و رمزنگاری‌اش می‌تونن اون رو بخونن چون جی میل از رمزنگاری سرتاسر پشتیبانی نمی‌کند. اما به محض دریافت ایمیل، پروتون میل اون رو با کلید عمومی کاربر رمزنگاری و سپس نگهداری می‌کند. از اون پس، پروتون میل 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.

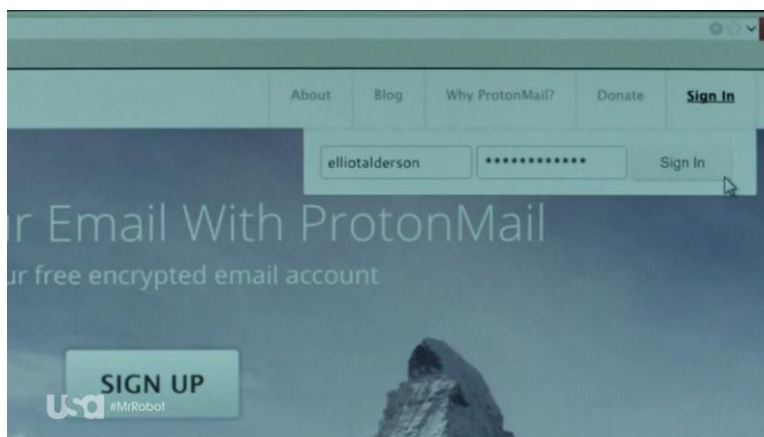
درمقابل، وقتی برای کاربر پروتون میل دیگه‌ای ایمیل ارسال می‌کنید، اون پیام روی دستگاه شما و با کلید عمومی گیرنده پیام رمزنگاری می‌شه، قبل از اینکه بخواد به دست پروتون میل برسه. در نتیجه، تنها فرستنده و گیرنده از محتوای باخبرن. این رمزنگاری سرتاسره.

بین رمزنگاری سرتاسر و رمزنگاری zero-access، اولی قوی‌تره از این جهت که پروتون میل به هیچ عنوان امکان دیدن پیام رو نداره. رمزنگاری zero-access از اصل داده شما در صورت نشت یا سرقت محافظت می‌کند، اما برای کسری از ثانیه (فاصله رسیدن پیام تا رمزنگاری) اون رو برای پروتون میل قابل دسترسی می‌کند. به همین خاطر، اگر پیامی با حساسیت بالا دارید، توصیه می‌شه دو طرف پروتون میل داشته باشن.

توجه کنید که پروتون میل یک ابزاره. فرقی نمی‌کند که در سوئیس. فرقی نمی‌کند که ادعا می‌کند امنیت و حریم خصوصی بهتری ارائه می‌ده. در نهایت، شما، به عنوان کاربر، در استفاده کارآمد ازش مسئولید.

مستر ربات

قبل از اینکه به جزئیات روش رمزنگاری پروتون میل پردازم، 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 پروتون میل در سریال مستر ربات (فصل اول، قسمت هشتم)

در فصل اول مستر ربات، الیوت رو می‌بینیم که از پروتون میل استفاده می‌کند. این جزئیات در نگاه اول کوچک و کم‌اهمیت به نظر میاد، اما داستان پشتش و مکالمه‌های مفصلی که سازندگان سریال با تیم پروتون میل در این باره داشتن نشون از توجه بالا به واقع‌گرایی و کیفیت بی‌نظیر نتیجه نهایی داره.

قسمت هشتم اوت ۲۰۱۵ به نمایش دراومد. [از قول تیم پروتون میل](#)، 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 پروتون میل از چنین امکانی پشتیبانی می‌کند.

Attempt	Time	IP
LOGIN SUCCESS	2015-05-08, 22:22:07	135.203.219.111
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
LOGIN FAILED	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, 18:10:46	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. الیوت 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.

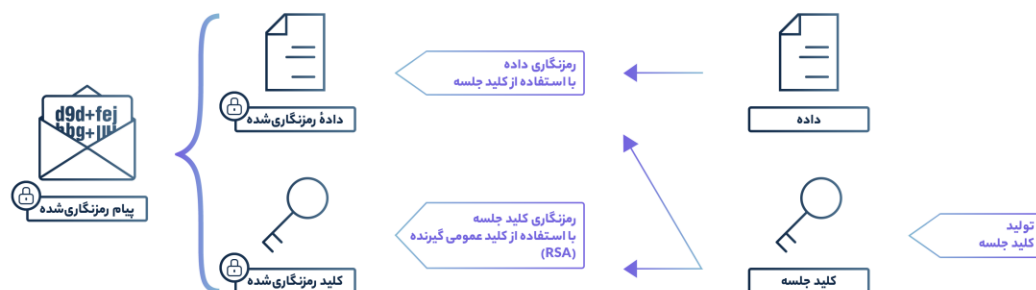
فکر می‌کنم آماده‌ایم تا به جزئیات رمزنگاری بپردازیم.

بهره‌مندی از PGP

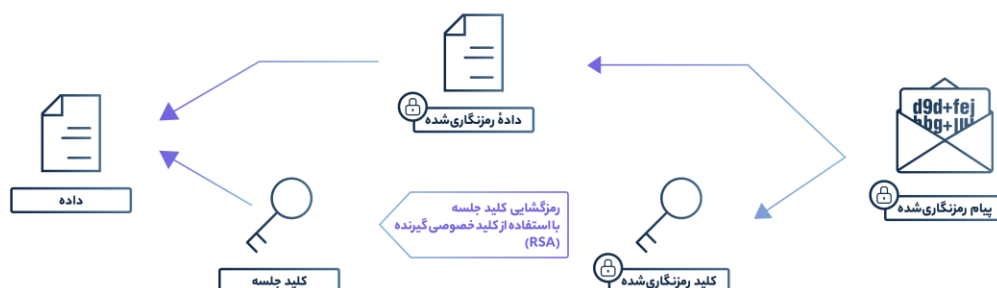
به‌طور خلاصه، پروتون میل از رمزنگاری PGP استفاده می‌کنه. در صورت عدم آشنایی با مفاهیم رمزنگاری، درک این بخش سخت خواهد بود. پیشنهاد می‌کنم ابتدا مطالب [رمزنگاری کلید عمومی RSA](#) و [راهنمای جامع PGP](#) رو مطالعه کنید و سپس به این بخش برگردید.

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.

رمزنگاری



رمزگشایی



اولین کاری که PGP انجام می‌دهد تولید یک کلید جلسه (session key) طولانی است. از این کلید برای رمزنگاری محتوای پیام (داده) استفاده می‌شود. کلید جلسه — که منحصر به فرد و با هر پیام تغییر می‌کند — سپس با کلید عمومی گیرنده رمزنگاری می‌شود.

به زبان ساده‌تر، پیام رو با استفاده از رمزنگاری متقارن و به کمک کلید جلسه رمز و به متنی غیر قابل 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 دارد، ابتدا کلید جلسه رو رمزگشایی و با کمک اون محتوای پیام رو باز می‌کند — سریع، امن، و بدون دردسر.

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

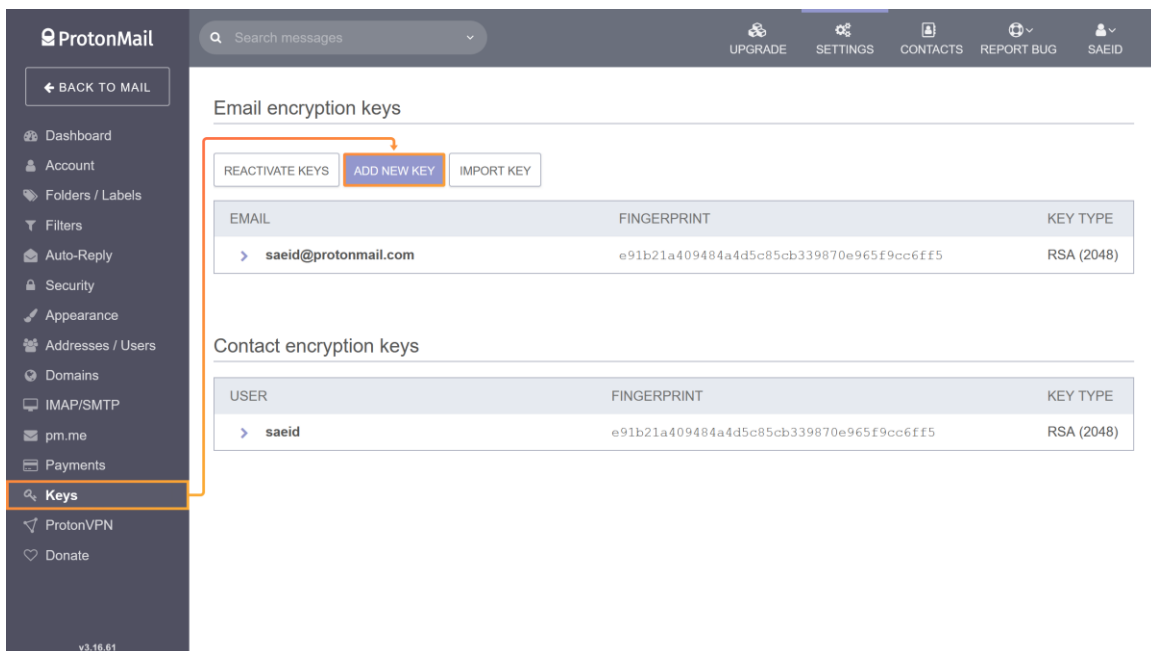
رمزنگاری کلید عمومی به‌طور کلی روش کندی محسوب می‌شود—بسیار کندتر از روش‌های متقارن. هرچقدر پیام و ضمیمه بلندتر و بزرگ‌تر باشد، رمزنگاری یا رمزگشایی اون‌ها زمان و قدرت پردازشی بیشتری می‌طلبد. روش فعلی سرعت و بهینگی رمزنگاری متقارن رو همراه با امنیت رمزنگاری کلید عمومی به ما می‌دهد.

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.

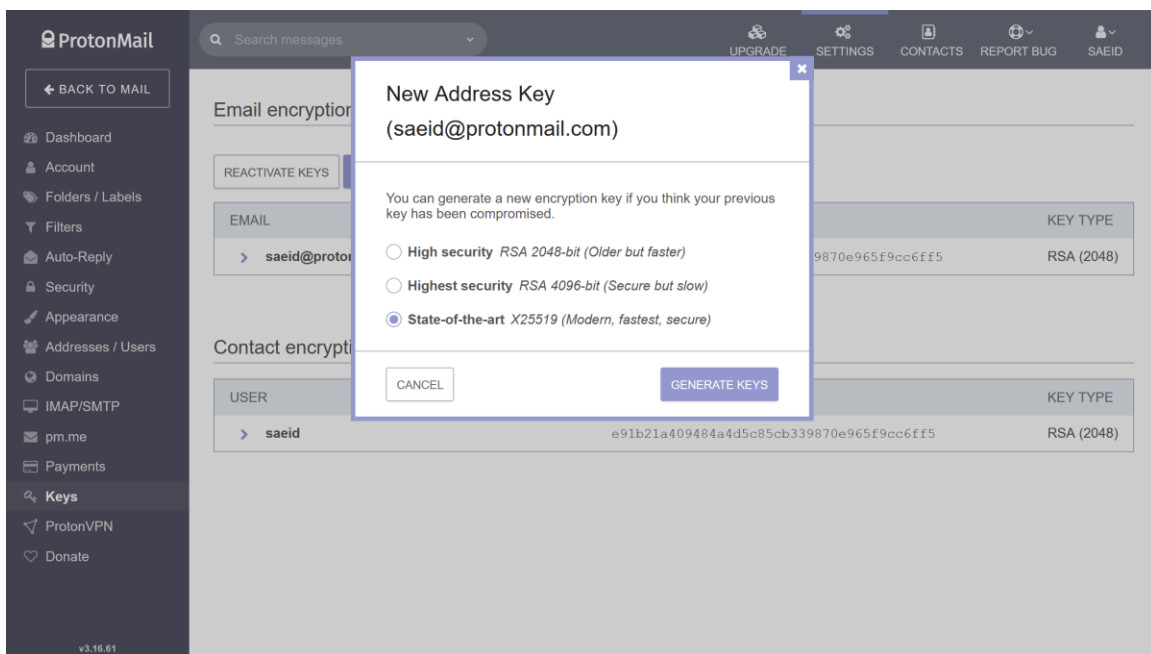
از طرفی، فرستنده چطور می‌تونه اعتماد کنه که کلید عمومی‌ای که برای رمزنگاری پیام و ارسالش به گیرنده استفاده می‌کنه به همون شخص تعلق داره؟ سرور می‌تونه یک کلید عمومی قلابی در اختیار فرستنده قرار بده. برای حل این مشکل، پروتون‌میل [احراز آدرس \(Address Verification\)](#) رو معرفی کرده. شما می‌تونید کلیدهای 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

ProtonMail

Search messages

UPGRADE SETTINGS CONTACTS REPORT BUG SAEID

BACK TO MAIL

Dashboard Account Folders / Labels Filters Auto-Reply Security Appearance Addresses / Users Domains IMAP/SMTP pm.me Payments

Keys

ProtonVPN Donate

v3.16.61

Email encryption keys

REACTIVATE KEYS ADD NEW KEY IMPORT KEY

EMAIL	FINGERPRINT	KEY TYPE
▼ saeid@protonmail.com	e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)

FINGERPRINT	KEY TYPE	STATUS	ACTIONS
e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)	PRIMARY ACTIVE	EXPORT
fe09e1b25b59ae6266b66893dbb4201a62f84d85	ECC (ed25519)	ACTIVE	EXPORT

Contact encryption keys

USER	FINGERPRINT	KEY TYPE
> saeid	e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)

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

ProtonMail

Search messages

UPGRADE SETTINGS CONTACTS REPORT BUG SAEID

BACK TO MAIL

Dashboard Account Folders / Labels Filters Auto-Reply Security Appearance Addresses / Users Domains IMAP/SMTP pm.me Payments

Keys

ProtonVPN Donate

v3.16.61

Email encryption keys

REACTIVATE KEYS ADD NEW KEY IMPORT KEY

EMAIL	FINGERPRINT	KEY TYPE
▼ saeid@protonmail.com	e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)

FINGERPRINT	KEY TYPE	STATUS	ACTIONS
e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)	PRIMARY	EXPORT
fe09e1b25b59ae6266b66893dbb4201a62f84d85	ECC (ed25519)	ACTIVE	EXPORT

MAKE PRIMARY

MARK OBSOLETE

MARK COMPROMISED

DELETE

Contact encryption keys

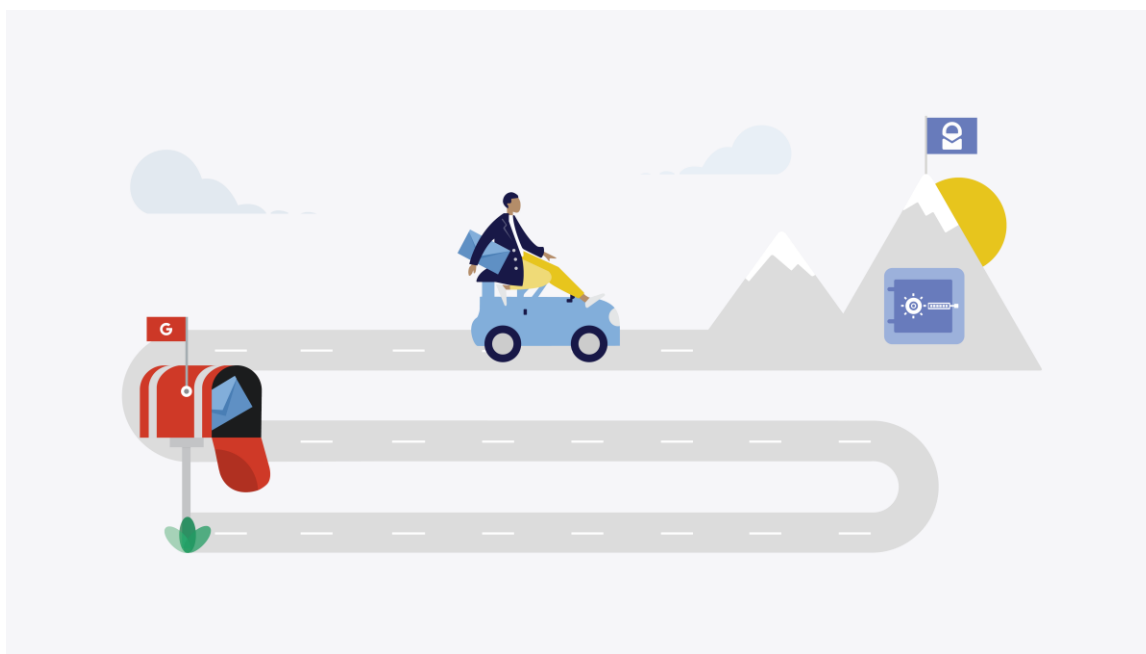
USER	FINGERPRINT	KEY TYPE
> saeid	e91b21a409484a4d5c85cb339870e965f9cc6ff5	RSA (2048)

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 سرویس‌های دیگه به پروتون‌میل

شما همچنین می‌تونید از سرویس‌های دیگه، مثل جی‌میل یا یاهو، به پروتون‌میل مهاجرت کنید، و نه تنها تمام ایمیل‌ها و فایل‌هاتون رو داشته باشید بلکه ایمیل‌های دریافتی در اون سرویس‌ها هم مستقیم به آدرس جدیدتون در پروتون‌میل 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 جی‌میل، ابتدا وارد تنظیمات جی‌میل شده و اطمینان حاصل کنید IMAP در بخش Forwarding فعاله. به Labels رفته و انتخاب کنید چه پوشه‌هایی رو می‌خواید انتقال بدید. به تصاویر صفحات بعد توجه کنید.

Settings

General Labels **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](#)

1. 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**

2. When messages are accessed with POP
keep Gmail's copy in the Inbox

3. 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

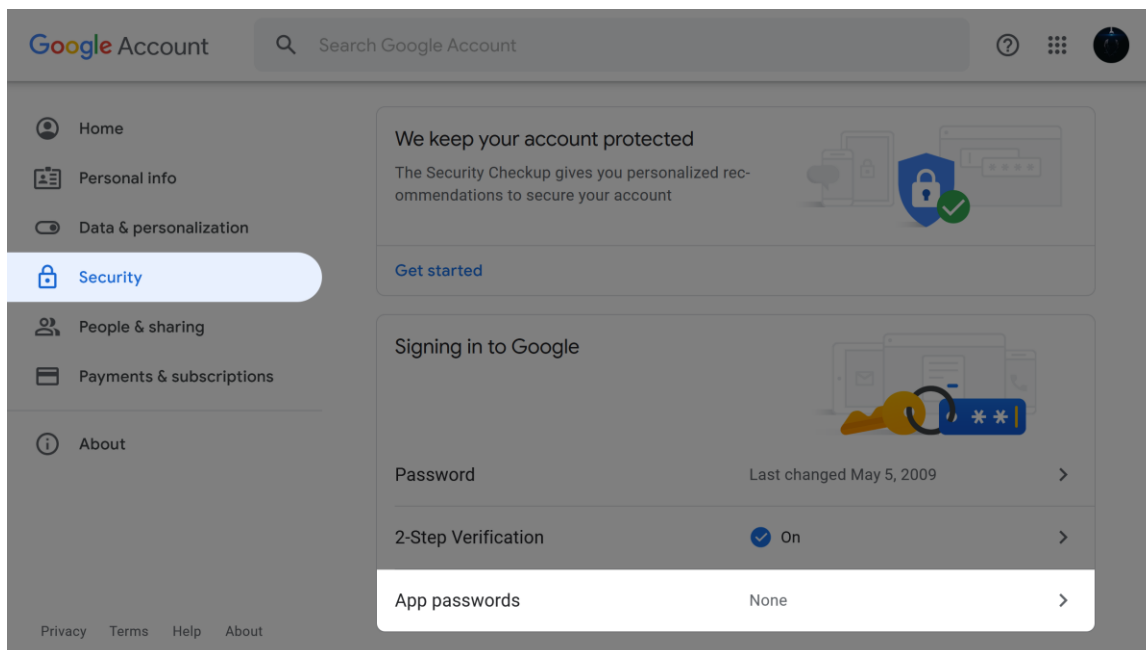
General **Labels** Inbox Accounts and Import Filters and Blocked Addresses

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

System labels	Show in label list
Inbox	<input checked="" type="checkbox"/> Show in IMAP
Starred	<input checked="" type="checkbox"/> Show in IMAP
Snoozed	<input checked="" type="checkbox"/> Show in IMAP
Important	<input checked="" type="checkbox"/> Show in IMAP
Chats	<input checked="" type="checkbox"/> Show in IMAP
Sent	<input checked="" type="checkbox"/> Show in IMAP
Scheduled	<input checked="" type="checkbox"/> Show in IMAP
Drafts	<input checked="" type="checkbox"/> Show in IMAP
All Mail	<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

Calendar

Contacts

YouTube

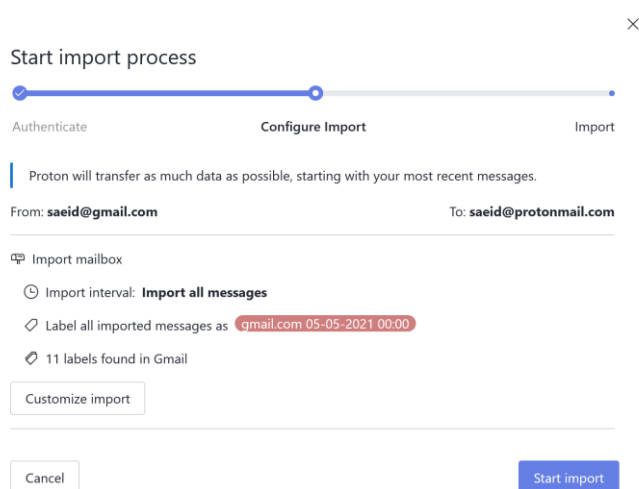
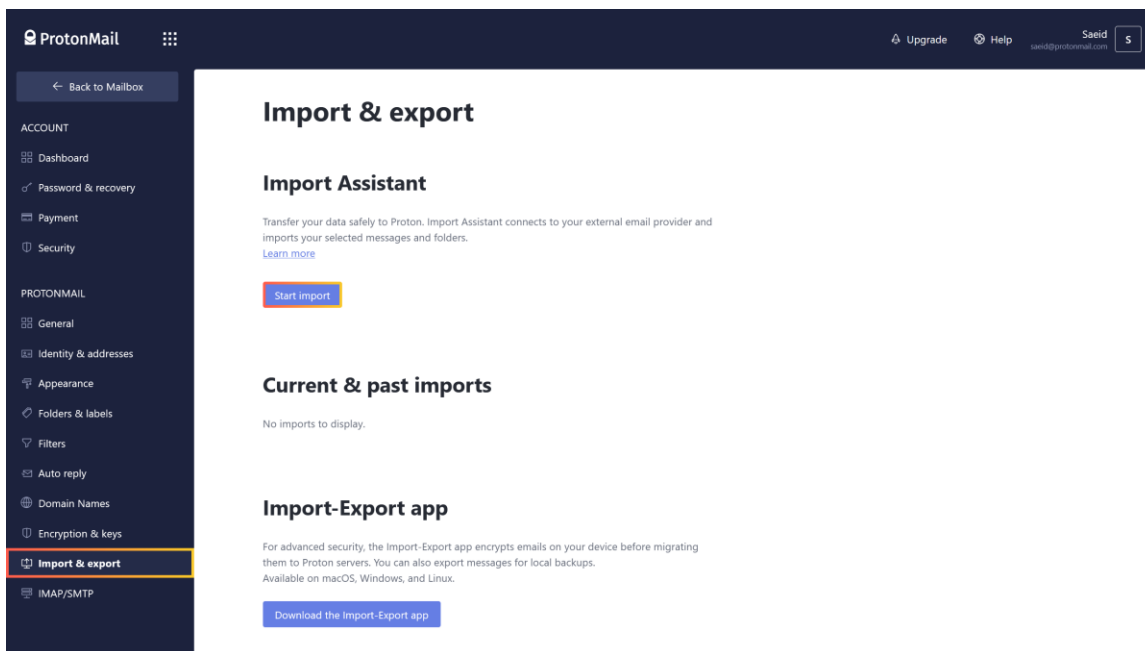
Other (Custom name)

GENERATE

Privacy Terms Help About

قدم سوم: تعیین رمز برای پروتون میل در Security → App passwords

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 بزنید. 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، [پرسید](#).

قدم آخر: Start import → Import Assistant

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 آدرس های موقت اشاره کردیم. ابزار [Firefox Relay](#) رو برای این کار در نظر داشته باشید. همچنین، از یک ایمیل برای همه ثبت نام ها استفاده نکنید.

برای ساختن حساب نیاز به وارد کردن شماره تلفن ندارید، اما اگر سرویسی از شما درخواست کرد، توجه داشته باشید که این موضوع حریم خصوصی شما رو تحت تأثیر قرار می ده. در صورت نیاز از شماره های مجازی استفاده کنید.

اگر بخوام یک منبع معرفی کنم که اطلاعاتتون رو کامل کنه، ویدئوی ارائه [بارت باتلر](#) مدیر ارشد تکنولوژی پروتون میله، که می تونید اون در [Vimeo](#) ببینید. در دقیقه دوازده، جایی که داره در مورد تجربه کاربری (UX) صحبت می کنه، نقل قول جالبی از بروس اشنایر (Bruce Schneier) میاره.

در نهایت، مهم ترین اصل اینه: DYOR (خودت تحقیق کن). پروتون میل بهترین نیست، اما گزینه خوبییه. [اشکال هایی بهش وارده](#)، و خوبه که بدونیم اون ها چی ان. بدون شک پیشرفت های زیادی داشته، اما بی نقص نیست. در نتیجه، تنها به حرف من اتکا نکنید، به خصوص وقتی پای امنیت و حریم خصوصی در میونه.

راهنماهای مرتبط



حریم خصوصی در فایرفاکس، ابزارها، و ترفندها



حریم خصوصی در عصر دیجیتال

