

# بسته کمک‌رسان پس‌کوچه



در شرایطی که کشورهای مختلف با اوضاع سیاسی و اجتماعی گوناگون دست و پنجه نرم می‌کنند، به عنوان نمونه مردم منطقه خاورمیانه که محدودیت‌های گوناگونی را از لحاظ آزادی‌های مدنی و سیاسی تجربه می‌کنند، و همچنین با توجه به شیوع گسترده ویروس کرونا، بیکاری بسیاری از افراد و وخیم‌تر شدن شرایط اقتصادی احتمال بروز اعتراضات مردمی بیش از پیش ارزیابی می‌شود.

پس‌کوچه به عنوان یک نهاد تخصصی و فنی فارغ از جهت‌گیری‌های سیاسی و اجتماعی، بسته‌ای پیشنهادی حاوی موارد مهم و لازم را به منظور بالا بردن آگاهی درباره حفاظت آنلاین و جلوگیری از دستگیری، بازداشت و در پی آن زندانی شدن و درگیر شدن با مسائل قضایی، برای کاربران تهیه کرده است.

آخرین به‌روزرسانی: ۳۰ آبان ۱۳۹۹



## بسته‌ی کمک‌رسان پس‌کوچه، شامل موارد زیر می‌شود:

- اقدامات دیجیتالی لازم برای حضور یافتن در مکان‌هایی که احتمال کنترل و نظارت بیرونی می‌رود و ممکن است امنیت شما به مخاطره بیفتد. ([برو به صفحه](#))
- بهترین روش‌ها برای مستند سازی، ارسال تصویر و ویدیو و مدارک و اسناد. ([برو به صفحه](#))
- آموزش نحوه دسترسی و ارتباط امن با کم‌ترین ریسک ([برو به صفحه](#))
- چگونگی برقراری ارتباط مطمئن هنگام قطعی اینترنت
- استفاده از ظرفیت‌های اینترنت در مواقعی که دسترسی به اینترنت به طور کامل ممکن نیست.



# ۱. اقدامات دیجیتالی لازم برای حضور یافتن در مکان‌هایی که احتمال کنترل و نظارت بیرونی می‌رود و ممکن است امنیت شما به مخاطره بیفتد.



## تلفن شما:



برای محافظت از حریم خصوصی و جلوگیری از نظارت و کنترل افراد، سازمان‌ها و نهادهای دیگر، بهترین کار این است که تلفن خود را در خانه بگذارید. به جای استفاده از تلفن شخصی، از یک تلفن دوم یا تلفنی که قابلیت منهدم شدن سریع داشته باشد، استفاده کنید.

### در صورت نیاز به تلفن شخصی‌تان، لطفاً مراحل زیر را دنبال کنید:

- اگر حتماً به حمل تلفن اصلی خود نیاز دارید، ترجیحاً آن را خاموش نگه دارید یا باتری تلفن را از جای خود خارج کنید و تا زمانی که نیاز به استفاده کامل از آن ندارید، باتری را داخل گوشی نگذارید. این کار پیگیری و کنترل فعالیت‌های شما را برای دیگران دشوار می‌کند.
- اگر برای مستندسازی هر رویدادی این الزام وجود دارد که تلفن شما روشن باشد، بهتر است که آن را در حالت هواپیما (Flight Mode) قرار دهید تا امکان ردیابی شما به حداقل برسد.

## حساب‌های کاربری در شبکه‌های اجتماعی:

از تمام حساب‌های کاربری خود در شبکه‌های اجتماعی خارج شوید یا برای اطمینان بیشتر اپلیکیشن‌های مربوط را به طور کامل از تلفن خود حذف کنید.

همچنین اگر با نام واقعی خود در شبکه‌های اجتماعی حضور دارید، توصیه ما حذف کامل این حساب‌های کاربری است تا نظرات و فعالیت‌های شما از خطر لو رفتن در امان باشد.

از سوی دیگر می‌توانید برای به اشتراک گذاشتن پست یا تصاویر و ویدیوها، حساب‌های کاربری جدید در شبکه‌های اجتماعی ایجاد کنید. به این ترتیب، کسانی که به دنبال رصد و کنترل حساب‌های مرتبط با شما هستند کار سخت‌تری برای شناخت هویت واقعی شما خواهند داشت.




## تلگرام:

اگر از پیام‌رسان تلگرام استفاده می‌کنید، اطمینان حاصل کنید که از گروه‌ها یا کانال‌هایی که می‌توانند برای شما خطرناک باشند، خارج شوید و آن‌ها را حذف کنید. اگر هم صاحب یک کانال یا گروه هستید، مدیریت آن را به شخص دیگری بسپارید، دسترسی‌های خود را به فرد مطمئن انتقال دهید و آن گروه یا کانال را از حساب کاربری خود حذف کنید.

## تهیه نسخه پشتیبان از تلفن خود:

حتماً از کلیه مدارک و اسناد، لیست مخاطبین، پیام‌های کوتاه، تصاویر و ویدیوها و سایر محتوای شخصی‌تان نسخه پشتیبان تهیه کنید. به یاد داشته باشید که از اپلیکیشن‌های پیام‌رسان که استفاده می‌کنید نیز یک نسخه پشتیبان تهیه کنید.

البته برای تهیه نسخه پشتیبان باید دقت کنید که این نسخه‌ها چه‌طور تهیه و کجا نگه داشته می‌شوند. چرا که نسخه پشتیبان به نوبه خود می‌تواند یک چالش از لحاظ امنیت اطلاعات شما باشد. 

اگر در این موارد نگرانی دارید یا از دانش کافی برای انجام صحیح آن برخوردار نیستید، بهتر است تمام نسخه‌های پشتیبان و اطلاعات موجود در آن‌ها را حذف کنید.

## اطلاعات حساس:

شواهد و مدارک مهم و حساس را (مثل ایمیل‌ها، پیام‌ها، تصاویر و ویدیوها) که ممکن است علیه شما یا دوستان‌تان استفاده شود، در صورت امکان حذف کنید. البته حذف پست‌ها و مدارک و اسناد نوشتاری و شنیداری و دیداری از حساب‌های کاربری فعال شما در شبکه‌های اجتماعی کمک بسیاری به امنیت بیشتر شما خواهد کرد.

## ایمیل:

توجه داشته باشید پس از حذف ایمیل‌های حساس، حتماً به پوشه مربوط به ایمیل‌های پاک شده (Junk یا Trash) مراجعه کنید و ایمیل‌ها را از آن‌جا نیز حذف کنید.



## قفل تلفن:

مطمئن شوید که قفل صفحه کلید روی تلفن شما فعال است. لطفاً از یک رمز عبور حداقل شش رقمی یا ترجیحاً یک عبارت عبور استفاده کنید. همچنین باید قفل‌های بیومتریک مانند ویژگی FaceID یا اثر انگشت را غیرفعال کنید و به جای آن از یک رمز عبور حداقل شش رقمی استفاده کنید.

## 🎧 میان‌برهای صفحه کلید دستگاه:

با استفاده از این ویژگی می‌توانید در حین استفاده از تلفن خود در مکان‌های عمومی و دانستن دکمه‌ها و میان‌برهای صفحه کلید در وقت خود صرفه جویی کنید. به عنوان مثال، از یک کلید میان‌بر برای روشن کردن دوربین یا ارسال پیام اضطراری استفاده کنید. این میان‌برها را بیاموزید و تمرین کنید، شاید بتوانید آن‌ها را به صورت دلخواه نیز تنظیم کنید. برای راهنمای بیشتر در این باره به [این صفحه](#) مراجعه کنید.

## 🔍 ویژگی «Find Your Phone»:

ویژگی «Find Your Phone» را طوری تنظیم کنید تا در صورت لزوم بتوانید تلفن خود را از راه دور پیدا کرده و اطلاعات آن را حذف کنید. بیشتر تلفن‌های هوشمند روشی مشخص را برای این کار ارائه می‌دهند. اطمینان حاصل کنید که با عملکرد آشنا هستید. در اینجا می‌توانید دستورالعمل‌های مربوط به سیستم عامل‌های [آی‌اواس](#) و [اندروید](#) را در اینجا ببابید.

## 📍 موقعیت مکانی تلفن:

در نظر داشته باشید که خدمات مربوط به موقعیت مکانی را در تلفن خود خاموش کنید. اگر می‌خواهید تصاویر یا اسنادی را پست کنید یا حساب کاربری شبکه‌های اجتماعی مانند توییتر و فیس‌بوک را به‌روزرسانی نمایید به اشتراک بگذارید بایستی خدمات موقعیت مکانی خود را برای این برنامه‌های به خصوص خاموش کنید.

## ۲. بهترین روش‌ها برای مستندسازی، ارسال تصویر، ویدیو، مدارک و اسناد



- در شرایطی که باید تلفن خود را همراه داشته باشید، از تماس‌های تلفنی و ارسال پیام‌های متنی به طور سنتی خودداری کنید. دسترسی به پیام‌های متنی شما آسان‌ترین روش کنترل تماس‌ها و محتوای ارتباط شما است. در هنگام افزایش خطر لو رفتن اطلاعات‌تان یا حضور در محل‌های عمومی نباید تصور کنید که پیام‌های شما خصوصی خواهند ماند.
- اگر باید برای ثبت هر رویدادی، تلفن خود را روشن کنید، بهتر است که آن را در حالت هواپیما بگذارید تا امکان ردیابی را به حداقل برسانید.
- سعی کنید که تا جای ممکن تلفن خود را همراه خود بیرون نبرید و با دوستان‌تان برای حضور در یک مکان خاص و در یک ساعت مشخص توافق کنید.
- اگر از یک فضای عمومی یا فرد به خصوصی عکس می‌گیرید و قصد دارید از آن‌ها در شبکه‌های اجتماعی استفاده کنید، اطمینان حاصل کنید که هیچ بخشی از چهره در آن وجود ندارد که بتواند به شناسایی افراد کمک کند. همچنین از سلفی گرفتن خودداری کنید.

### اپلیکیشن‌های امن برای مستندسازی و گزارش دهی

#### اپلیکیشن تلا (Tella)

«تلا» یک اپلیکیشن مستندسازی برای سیستم‌عامل اندروید است. این اپلیکیشن، ثبت اسناد و مدارک مربوط به رویدادها را در محیط‌های ناامن -با اتصال اینترنتی محدود یا بدون اینترنت یا در مواجهه با سرکوب- آسان‌تر و ایمن‌تر می‌کند.

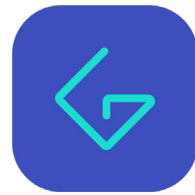


دانلود اپلیکیشن Tella از پس‌کوچه



## اپلیکیشن حافظ

اپلیکیشن چند کاربردی حافظ، حاصل تلاش مشترک خبرگزاری هرانا، وابسته به مجموعه فعالان حقوق بشر در ایران و سازمان اتحاد برای ایران طی پروژه ایران کوباتور برای توسعه جامعه مدنی است.



حافظ، اپلیکیشنی است که امنیت شما را در نظر می‌گیرد و قرار است حافظ گردش آزاد اطلاعات در ایران باشد. حافظ را به عنوان اپلیکیشنی که تست‌های امنیتی خود را به خوبی طی کرده و دارای وابستگی و هویت حقوقی روشنی به نهادهای مدافع حقوق بشر با سابقه است در نظر بگیرید.

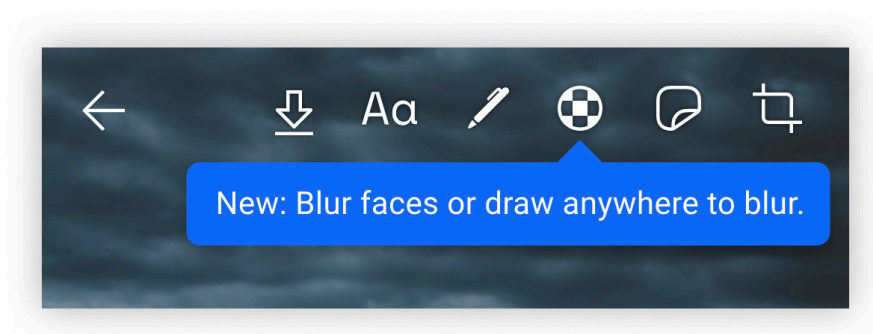
این اپلیکیشن چند کاربردی در مهمترین ویژگی خود قابلیت ثبت و ارسال امن گزارش‌های خبری، تصویری، صوتی و ویدیویی شما را دارد. تاریخچه‌ی فعالیت شما و نیز اطلاعات تماس شما در هیچ‌جا توسط این برنامه جمع‌آوری یا ذخیره نمی‌شود، حتی گیرندگان گزارش‌ها نیز به اطلاعات کاربری یا تماس شما دسترسی ندارند.

دانلود اپلیکیشن Hafez از پس‌کوچه

دریافت اپلیکیشن Hafez از طریق ایمیل

## برنامه تار شدن چهره:

گر شما به طور ناخواسته از چهره افراد عکس گرفتید، اپلیکیشن‌هایی وجود دارند که به شما در مات کردن چهره‌ها کمک می‌کنند. به عنوان مثال **سیگنال** در نسخه جدید خود برای این کار امکان جدیدی را اضافه کرده است.



## ۳. آموزش نحوه‌ی دسترسی و ارتباط امن با کم‌ترین ریسک



در ادامه تعدادی از پیام‌رسان‌ها و فیلترشکن‌های امن را به شما معرفی خواهیم کرد که می‌توانید از آن‌ها برای برقراری ارتباط مطمئن در مواقعی که احتمال سانسور گسترده و یا قطعی اینترنت وجود دارد، استفاده کنید.

### چگونگی برقراری ارتباط مطمئن هنگام قطعی اینترنت

در اینجا قطعی اینترنت به این معنا قطع اینترنت به طور کلی است. یعنی حتی امکان استفاده از اینترنت داخلی هم وجود ندارد. در این شرایط تنها راه اتصال از طریق تکنولوژی‌هایی مثل bluetooth یا شبکه wifi محلی امکان پذیر است.

#### پیام‌رسان Briar:

شما می‌توانید هنگام قطع شدن‌های جزئی و کلی اینترنت، با استفاده از اپلیکیشن Briar و با اتصال به وای‌فای یا بلوتوث به طور امن با دیگران ارتباط برقرار کنید.



#### محدودیت‌های Briar:

۱. کاربران Briar برای استفاده از دامنه‌های وای‌فای و بلوتوث محدود هستند.
۲. این اپ به عنوان راه‌حل جایگزین، از شبکه تور برای ارتباط دامنه‌های بالاتر استفاده می‌کند. اگر شبکه تور مسدود شود، کاربران بایستی فقط از طریق پل‌های شبکه تور (Tor Bridges) اتصال برقرار کنند.

دانلود Briar از پس‌کوچه



دریافت Briar از طریق ایمیل



راهنمای استفاده از پیام‌رسان Briar



## استفاده از ظرفیت‌های اینترنت در مواقعی که دسترسی به اینترنت به طور کامل ممکن نیست

### پیام‌رسان Jami:

هنگامی که یک اتصال اینترنتی عادی وجود دارد و شما دوست دارید به جای انتقال اطلاعات خود از طریق یک سرور متمرکز، از روش رمزگذاری کاربر به کاربر (Peer to Peer) استفاده کنید، می‌توانید از پیام‌رسان Jami استفاده کنید. همچنین هنگامی که دسترسی به اینترنت جهانی ممکن نیست ولی اتصال اینترنتی در داخل کشور امکان‌پذیر است، با استفاده از Jami می‌توانید یک ارتباط امن و رمزگذاری شده با دیگران داشته باشید. به عنوان مثال، اگر در تهران ساکن هستید و قصد دارید تا با شخصی در اهواز ارتباط برقرار کنید، Jami می‌تواند این ارتباط را به صورت امن انجام دهد.



### محدودیت‌های Jami:

۱. Jami برای اینکه یک ابزار مناسب و مفید باشد، نیاز به تعداد زیادی کاربر دارد.
۲. اپلیکیشن Jami ارتباط آفلاین را پشتیبانی نمی‌کند. البته امکان ارتباط با افراد نزدیک به شما از طریق یک شبکه محلی وجود دارد.

راهنمای استفاده از پیام‌رسان Jami

دانلود Jami از پس‌کوچه

### دانلود اپلیکیشن از طریق ایمیل:

دریافت Jami برای اندروید

دریافت Jami برای ویندوز

دریافت Jami برای مک

دریافت Jami برای آی‌اواس

دریافت Jami برای لینوکس












































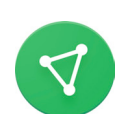














به شما پیشنهاد می‌کنیم برای انتخاب یک فیلترشکن خوب، خصوصیات زیر را در نظر بگیرید:

۱. سازندگان فیلترشکن موردنظر نسبت به ذخیره اطلاعات و فعالیت‌های آنلاین کاربران حساس باشند.
۲. متن‌باز باشد.
۳. سند حریم خصوصی و وبسایت رسمی و قانونی داشته باشد.
۴. از راه‌های مختلف برای دور زدن فیلترینگ استفاده کند.
۵. پشتیبانی قدرتمند و سریع داشته باشد و به‌روزرسانی منظم انجام دهد.
۶. از تکنیک‌های رمزگذاری مدرن و به‌روز استفاده کند.
۷. تست‌های تخصصی و فنی را با موفقیت پشت سر گذاشته باشد.



## دانلود فیلترشکن‌ها (از طریق کانال تلگرام یا با فرستادن یک ایمیل خالی)

تیم پس‌کوچه به شما پیشنهاد می‌کند که فیلترشکن‌های زیر را از **طریق تلگرام یا ایمیل برای سیستم‌عامل‌های مختلف** دانلود و در مواقع ضروری از آن‌ها استفاده کنید. برای اطلاعات بیشتر درباره هر کدام از آن‌ها به لینک‌های موجود مراجعه کنید.

 لینوکس	 لینوکس ۳۲	 مک	 ویندوز	 اندروید	 Tor	 اندروید	 تلگرام	 Orbot				
						 تمام سیستم‌عامل‌ها	 تلگرام	 Outline				
 لینوکس	 لینوکس ۳۲	 مک	 ویندوز	 آی‌اواس	 اندروید	 تلگرام	 Lantern					
						 لینوکس	 مک	 ویندوز	 آی‌اواس	 اندروید	 تلگرام	 Windscribe
 لینوکس	 مک	 ویندوز	 اندروید	 Riseup VPN	 ویندوز	 اندروید	 تلگرام	 Windscribe				
					 ویندوز	 اندروید	 تلگرام	 ProtonVPN				
						 لینوکس	 مک	 ویندوز	 اندروید	 تلگرام	 Geph	
 اندروید	 تلگرام	 Your Freedom	 ویندوز	 آی‌اواس	 اندروید	 تلگرام	 TunnelBear					



## توشه سرویس ماهواره‌ای و اپلیکیشن توشه:

توشه یک سرویس انتقال یک طرفه اطلاعات از طریق ماهواره است. با استفاده از این سرویس می‌توانید حتی در مواقع قطع کامل اینترنت، محتوای اینترنت و همچنین فضای رسانه‌ای اعم از دیداری و شنیداری را بدون پرداخت هیچ هزینه‌ای و از طریق فقط یک رسیور بگیرید و فایل‌های دریافت شده را استخراج کرده و در دستگاه‌های اندرویدی خود مشاهده کنید.

با شبکه ماهواره ای توشه در واقع می‌توانید هر روز چندین گیگابایت محتوا را با سرعت بالا از گیرنده ماهواره خانگی دریافت و روی کامپیوتر، تبلت یا تلفن همراه استفاده کنید. حتی اگر مشکل کمبود سرعت اینترنت دارید و سایت‌ها فیلتر هستند با استفاده از توشه برنامه‌های متنوع، بدون سانسور و فیلتر در دسترس شما خواهد بود. برای استفاده از توشه نیازی به اشتراک ماهانه نیست استفاده از این سرویس برای کاربران کاملاً رایگان و بدون هزینه است.

معرفی کوتاه توشه به صورت ویدیویی

راهنمای استفاده از توشه

همچنین در هنگام قطع اینترنت و قطع شدن دسترسی کاربران به اینترنت جهانی، با استفاده از اپلیکیشن توشه علاوه بر اطلاع از اخبار و اطلاعات مهم روز، می‌توانید فیلترشکن‌ها، نرم‌افزارهای پیام‌رسان و آنتی‌ویروس‌های آماده شده توسط پس‌کوچه را نیز دریافت کنید.



لینوکس



ویندوز



اندروید

دانلود توشه از پس‌کوچه

در حال حاضر شبکه توشه بر روی ماهواره یاهست و در فرکانس زیر در دسترس است:

فرکانس: ۱۱۷۶۶

سیمبل ریت: ۲۷۵۰۰ عمودی

## منابع و لینک‌های مفید

- <https://irandarkhamooshi.net/fa>
- <https://www.article19.org/fa/ttn-iran-november-shutdown-2>
- <https://iran-shutdown.amnesty.org>
- <https://www.instagram.com/p/CA5b2Dkg9VI/>
- [https://twitter.com/evan\\_greer/status/1266907704850857984](https://twitter.com/evan_greer/status/1266907704850857984)
- <https://tech.tavaana.org/fa/news/nkat-amnyty-drwry-bray-shrkt-dr-rahpy-mayy-w-tjm>
- [https://www.amnestyusa.org/pdfs/SafetyDuringProtest\\_F.pdf](https://www.amnestyusa.org/pdfs/SafetyDuringProtest_F.pdf)
- <https://www.itspronouncedmetrosexual.com/2017/01/a-few-small-tips-for-attending-your-first-protest-march/>
- <https://www.bustle.com/p/how-to-reduce-cybersecurity-risks-when-attending-protests-22947973>
- <https://ssd.eff.org/en/module/attending-protest>
- <https://www.forbes.com/sites/krisholt/2020/06/07/privacy-black-lives-matter-protest-george-floyd/#2ca6a3541801>
- <https://theintercept.com/2017/04/21/cybersecurity-for-the-people-how-to-protect-your-privacy-at-a-protest/>
- <https://www.amnesty.org/en/latest/campaigns/2020/06/tactics-to-secure-phone-before-a-protest/>
- [https://www.vice.com/en\\_us/article/gv59jb/guide-protect-digital-privacy-during-protest](https://www.vice.com/en_us/article/gv59jb/guide-protect-digital-privacy-during-protest)

