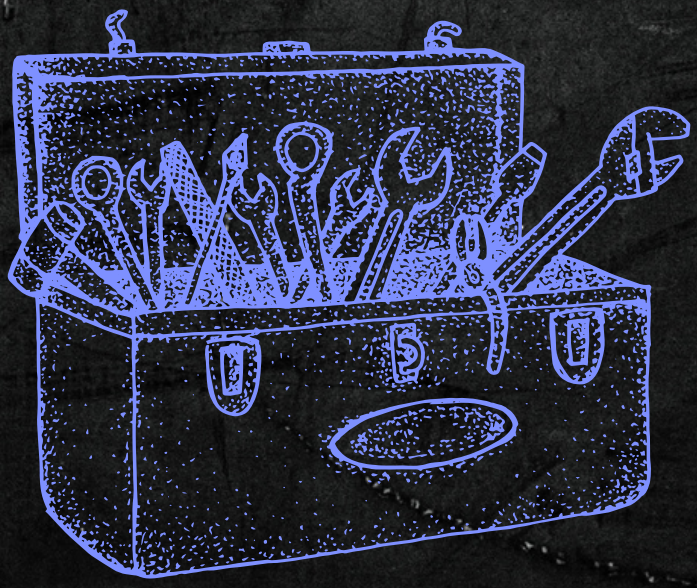
FILTER WATCH



جعبه ابزارهای خاموشی

www.irandarkhamooshi.net

ایران در خاموشی

پیش درآمد

آخرین به روزرسانی: ۱۴۰۱/۰۷/۲۵

به «ایران در خاموشی» خوش آمدید،
وبسایت ایران در خاموشی قرار است به شما کمک کند تا پیش از آنکه دیر شود، خودتان را برای قطعی یا اختلال‌های احتمالی اینترنت آماده کنید.
مدتهاست که پژوهشگران دربارهی توانایی دولت ایران در محدود کردن دسترسی به اینترنت، هشدار میدهند. ایران با پیش بردن طرح موسوم به صیانت از فضای مجازی و از طریق قرار دادن محتوا و خدمات اصلی بر روی شبکه ملی اطلاعات (یا همان اینترنت ملی)، مشغول ساختن زیرساختهای لازم برای قطع ارتباط کاربران با شبکه جهانی اینترنت است.
آبان ۱۳۹۸ بود که دولت ایران برای نخستین بار این قابلیت خود را به نمایش گذاشت؛ در واکنش به موج اعتراضات سراسری در کشور، ایران شاهد قطعی تقریبا کامل اینترنت بود که گردش اطلاعات را از بیرون به کشور و از کشور به بیرون به شدت محدود کرده بود.
از ۲۵-۲۴ آبان ، دسترسی به اینترنت جهانی به طور وسیعی قطع شد. این قطعی کامل اینترنت به مدت یک هفته ادامه داشت تا زمانی که از ۲-۱ آذر ماه به بعد، بخش محدودی از اتصال اینترنتی در بیشتر استانها (و نه تمام آنها) از سر گرفته شد.
در زمان این قطعی اینترنت، ارتباط از طریق اپلیکیشنهای معمول پیامرسان، دسترسی به اطلاعات از طریق اینترنت جهانی و یا به اشتراک گذاشتن محتوا روی شبکههای اجتماعی تقریبا غیرممکن بود.
این قطع شدن اینترنت، حقوق بنیادین بشر را نقض کرد، زندگی مردم را مختل نمود، و به صورت جدی به اقتصاد دیجیتال صدمه زد.
از آن تاریخ، با انتقال سرور ادارات دولتی، بانک‌ها و کسب و کارهای دیجیتال بر روی سرورهای داخلی، حمایت و تقویت اپلیکیشن‌ها و پیام‌رسان‌های تولید داخل و اختصاص بسته‌های تشویقی برای استفاده کنندگان از پهنای باند داخلی به منظور سو دهی به رفتار کاربران، توان حاکمیت در قطع کم هزینه‌تر اینترنت جهانی به مراتب بیشتر شد.
همگام با گسترش اعتراضات مدنی و معیشتی، کاربران در ایران دست کم هفت بار دیگر و به مدت زمان‌های مختلفی با قطع کامل اینترنت مواجه شده‌اند:
در دی ۹۸ به مدت ۱۵ دقیقه و به شکل سراسری، تیر ۹۹ به مدت دو ساعت در بهبهان، اسفند ۹۹ به مدت سه روز در سیستان و بلوچستان، خرداد ۱۴۰۰ به مدت ۱ روز در یاسوج، تیر۱۴۰۰ به مدت ۶ روز در خوزستان، آبان ۱۴۰۰ به مدت ۲ روز در اهواز و آبان ۱۴۰۰ به مدت ۱ روز در اصفهان.
همچنین در اردیبهشت ۱۴۰۱ و در خلال اعتراضات خوزستان نیز اینترنت در ساسر این استان با اختلالات گسترده و نزدیک به قطعی اینترنت مواجه بود هاست.
این اتفاقی است که به سادگی ممکن است تکرار شود. مسئولین دولتی در ایران حالا بیش از هر زمانی آماده قطع دوباره اینترنت در ایران هستند، بنابراین مهم است که شما نیز برای چنین اتفاقی آماده باشید. بدون شک آمادگی بیشتر مردم، تاثیرگذاری این اتفاق را کمتر خواهد کرد.

معرفی جعبه ابزارهای قطع اینترنت

«ایران در خاموشی» چهار جعبه‌ابزار قطع اینترنت تهیه کرده است که می‌توانید آن‌ها را در جایی امن دانلود و ذخیره کنید تا در صورت قطعی اینترنت، در دسترس داشته باشید.
بسیاری از این ابزارها از فناوری‌هایی استفاده می‌کنند که هنوز جدید و ناآشنا هستند و در موقعیت‌های واقعی امتحان نشده‌اند. به همین دلیل نمی‌توان به صورت قطعی و روشن پیشنهاد کرد که در شرایطی که ارتباط اینترنتی، محدود و یا کاملا قطع است، کدام یک از آن‌ها خوب عمل می‌کنند.
ما در این بخش سعی می‌کنیم تا نقاط قوت بالفعل این ابزارها را نشان بدهیم و در عین حال خطرات امنیتی و ناشناخته‌های بعضی از این ابزارها را نیز مشخص کنیم.

این چهار جعبه‌ابزار شامل **جعبه‌ابزار روزمره**، **جعبه‌ابزار اختلال**، **جعبه‌ابزار قطع اینترنت** و **جعبه‌ابزار خاموشی کامل** است. از طریق این چهار جعبه‌ابزار می‌توانید ابزارهایی که در حال حاضر برای دستیابی به اطلاعات در حالت روزمره، در هنگام قطعی بخشی از اینترنت، و یا قطعی کامل اینترنت در دسترس هستند استفاده کنید.

جعبه‌ابزار روزمره شامل ابزارهایی برای استفاده روزمره است که شما می‌توانید برای ایمن نگه‌داشتن مکاتبات و تماس‌های خود، یا دور زدن فیلترینگ‌های معمول، و همین‌طور برای جلوگیری از افشای نام خود در فضای آنلاین از آن‌ها بهره ببرید. اما حواستان باشد که بسیاری از ابزارهای این جعبه، در زمان قطع اینترنت موثر نیستند.

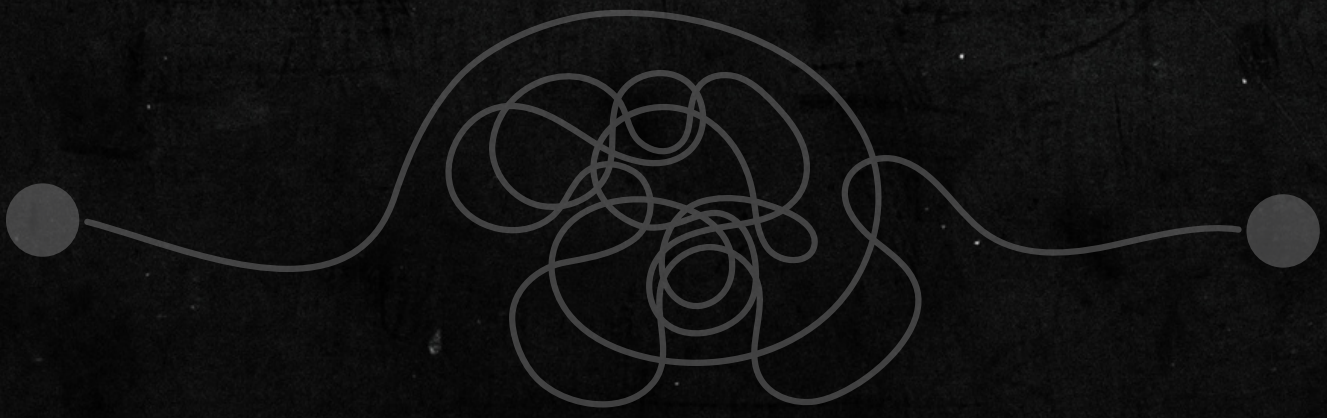
جعبه‌ابزار اختلال در اینترنت می‌تواند در زمانی که ارتباط اینترنتی شما دچار اختلال می‌شود به کار بیاید. ابزارهای این جعبه طوری طراحی شده‌اند که به شما اجازه می‌دهند بتوانید در شبکه‌های اجتماعی فعال بمانید و به محض وصل شدن اینترنت، اطلاعات و اخبار را به مخاطبان و دوستان خود برسانید.

جعبه‌ابزار قطع اینترنت ابزارهایی دارد که در زمان قطع طولانی مدت اینترنت، مانند اتفاقی که در آبان ماه ۱۳۹۸ رخ داد، قابل استفاده هستند. در این مورد به‌خصوص، وقتی دسترسی به اینترنت جهانی محدود شده بود، اینترنت ملی همچنان قابل دسترسی بود. ابزارهای این جعبه به شما اجازه می‌دهند تا با جهان خارج از کشور در ارتباط بمانید و به اطلاعات دسترسی داشته باشید.

جعبه‌ابزار خاموشی کامل شامل ابزاری است که ممکن است در زمان قطع کامل اینترنت، وقتی که حتی شبکه اینترنت ملی هم محدود شده، به کار بیاید.

طرز کار با بعضی از این ابزارها ممکن است کاملاً سرراست نباشد و شما برای اینکه بخواهید به شکلی امن و موثر از آن‌ها استفاده کنید نیاز به راهنما و توضیح داشته باشید. به همین منظور، ما راهنماهایی را که در حال حاضر برای این ابزار موجود است، گرد هم آورده‌ایم.
«ایران در خاموشی» در چند ماه آینده راهنماهای بیشتری را برای آمادگی در برابر قطعی اینترنت منتشر خواهد کرد.
تاکید می‌کنیم که ابزارهایی که در این‌جا منتشر کرده‌ایم ابزارهایی هستند که پژوهشگران ما آن‌ها را موثرترین روش‌ها برای برقرار نگه‌داشتن ارتباط و دسترسی به اطلاعات در زمان قطعی اینترنت، می‌دانند.

لطفاً به این موضوع توجه کنید که تمام این ابزارها لزوما در زمینه ی حفظ امنیت دیجیتال،ناشناس ماندن و حفظ حریم خصوصی شما، به درستی عمل نخواهند کرد. ما ابزارهایی را که خطر ناامنی حریم شخصی در آنها شناسایی شده، مشخص کرده‌ایم، و توصیه می کنیم در مواقع بحرانی، با احتیاط زیاد از آنها برای برقراری ارتباط و دسترسی به اطلاعات استفاده کنید.
اگر شما از این ابزارها استفاده کرده اید، یا اگر خودتان در این زمینه تحقیق می کنید، مشتاقیم که نظرات شما را درباره ی امنیت وکارایی این ابزار در موقعیت های قطع اینترنت بشنویم. میتوانید نظرات خود را در بخش تجربیات شما با ما در میان بگذارید.



درباره‌ی ما

«ایران در خاموشی» چیست؟

اگر می‌خواهید در زمان قطع اینترنت ارتباط خود را با مخاطبان، دوستان و دنیای بیرون حفظ کنید، بسیار مهم است که از قبل آماده باشید.

زمانی که دیگر ارتباط شما با اینترنت جهانی قطع شده، گزینههای موجود بسیار محدودتر خواهد بود. دیگر نمیتوانید ابزار یا اپلیکیشنی دانلود کنید، یا روی اینترنت به دنبال دستورالعملهای لازم برای اتصال بگردید.

اگر میخواهید ارتباط و اتصال خود را حفظ کنید، از الان باید برنامهریزی را شروع کنید.

گروه «ایران در خاموشی» تلاش کرده است تا ابزارهای موجودی را که ادعا میکنند در زمان قطع یا اختلال اینترنت پایدار هستند، پیدا کند. ما این ابزارها را در قالب چهار جعبه ابزار به منظور استفاده در چهار موقعیت مختلف ارائه می‌دهیم.

البته تمام این ابزارها در نهایت به شکل کامل کارایی نخواهند داشت، همهی آنها برای استفاده در زمان قطعی اینترنت در ایران مناسب نخواهند بود و ما خطرات و نگرانیهای مربوط به این ابزارها را - هر جا که این خطرات برایمان قابل شناسایی باشند - مشخص خواهیم کرد.

بدین ترتیب وبسایت ایران در خاموشی، دستورالعمل و راهنمای ساده‌ی استفاده از ابزارها را جمع‌آوری کرده و در ماه‌های آینده نیز راهنماهای بیشتری برای آمادگی در برابر قطعی اینترنت منتشر خواهد کرد. همچنین و گاه به گاه این جعبه ابزارها به روزرسانی خواهند شد تا جدیدترین نسخه از برنامه‌های پیشنهادی را ارائه و یا ابزارهای نوظهوری را اضافه کنند. ما همچنین تمام جعبه ابزارهای وبسایت را یک جا و در جعبه ابزار آفلاین، به زبان دیگر قومیت‌های ساکن در ایران از جمله بلوچی، ترکی، کردی و عربی ترجمه کرده‌ایم تا این ابزار در اقصی نقاط ایران در دسترس کاربران قرار گیرد.

اگر علاقه‌مند هستید و حاضرید درباره هر کدام از ابزارهایی که «ایران در خاموشی» ارائه می‌دهد، بازخورد و نظر خود را به ما منتقل کنید، بسیار قدردان کمک شما خواهیم بود. می‌توانید نظرات خود را در بخش تجربیات شما اضافه کنید.

ما همچنین کتابخانه‌ای از منابع در بخش مرکز اطلاعات در اختیار شما می‌گذاریم که در زمینه‌ی راه‌های برنامه‌ریزی پیش از اختلال و کاهش تأثیرات قطع شدن و اختلال اینترنت به شما کمک می‌کنند. این مرکز منابع، حاصل کار تعدادی از متخصصان و موسسات امنیت دیجیتال را یک‌جا جمع‌آوری می‌کند تا توصیه‌های مهمی درباره اینکه چگونه امنیت خود را حفظ کنید و در عین حال در زمان قطع اینترنت به اطلاعات و افراد دسترسی داشته باشید، به شما ارائه دهد.

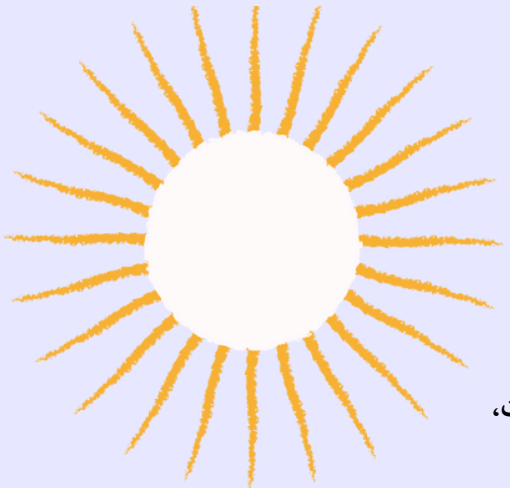
در این بخش همچنین برای هر ابزاری که در جعبه ابزارهای مختلف وبسایت معرفی شده است، یک راهنمای آموزشی ساده‌ی نصب و استفاده در نظر گرفته شده است تا به وسیله آن هر فردی با هر میزان دانش دیجیتال بتواند از این ابزارها در زمان خاموشی اینترنت بهره ببرد.

چرا قطع اینترنت خطرناک است؟

قطع شدن اینترنت و اختلال در آن، به شکلی بنیادین حقوق بشر را هم در فضای آنلاین و هم در دنیای واقعی نقض میکند.
علاوه بر محدود کردن حق بنیادین آزادی بیان شهروندان، قطع اینترنت پردهای از تاریکی ایجاد میکند که در پس آن سرکوب، بازداشتها و خشونت حکومت که در فضای واقعی صورت گرفته، پنهان میشود.
این نوع تخطیها در پشت این پرده تاریک رخ میدهند، بدون آنکه شهروندان بتوانند آنها را ثبت کنند، در فضای آنلاین به اشتراک بگذارند و یا از آنها به عنوان مدرکی استفاده کنند تا مسئوالن مجبور به پاسخگویی شوند.

پروژهی «ایران در خاموشی» را چه کسانی اداره میکنند؟

ایران در خاموشی پروژهای است که سازمان میان گروه آن را اداره میکند. این وبسایت برای نخستین بار توسط سازمان Small Media راهاندازی شده بود.
این پروژه بدون حمایت و همکاری تعداد زیادی از متخصصین این حوزه امکانپذیر نبود و ما از همکارانمان در«پسکوچه»، «توشه» و «فمینیست اسپکتروم» در کنار بسیاری افراد دیگر، به خاطر مشارکت در این پروژه سپاسگزاری میکنیم.



جعبه‌ابزار روزمره

شما نباید فقط در زمان‌های حساس و بحرانی نگران امنیت دیجیتال و حریم خصوصی خود باشید. در جعبه‌ابزار روزمره‌ی ما، توصیه‌هایی درباره‌ی شیوه کار با یک سری ابزار وجود دارد که می‌توانید همیشه، و نه لزوماً زمان به‌وجود آمدن اختلال در اینترنت، برای امور روزمره از آن‌ها بهره ببرید.

این ابزارها شامل اپلیکیشن‌های مطمئن پیام‌رسان هستند که برای محافظت گفتگوهای شما در برابر دستگاه‌های شنود دولتی و شرکت‌های خصوصی طراحی شده‌اند؛ همچنین وی‌پی‌ان‌ها و پروکسی‌هایی که می‌توانند در حفظ امنیت شما در فضای آنلاین و گذر از فیلترهای دولتی بکار بیایند.

همیشه به خاطر داشته باشید که استفاده از چنین ابزاری، در صورتی که مسئولان حکومتی آن‌ها را روی دستگاه‌های شما پیدا کنند، می‌تواند ایجاد سوءظن کرده و شما را به خطر بیندازد، پس با احتیاط عمل کنید.

ما راهنمای مهمی درباره محاسبه و تشخیص ریسک‌های فضای آنلاین داریم که به شما کمک می‌کند تا اقدامات امنیتی مناسب برای خود را بشناسید. به شدت توصیه می‌کنیم تا این راهنما را قبل از ادامه دادن این مطلب مطالعه کنید.

اپلیکیشن‌های پیام‌رسان – به طور امن گفتگو و مکاتبه کنید!

یک سری مسائل بنیادی وجود دارند که همه‌ی ما باید برای محافظت از خودمان، دوستان و خانواده‌مان در نظر بگیریم.

مهم‌ترین (و ساده‌ترین) کاری که شما همین امروز می‌توانید انجام دهید تا از خود و از تمام کسانی که با آنها در ارتباط هستید، محافظت کنید، این است که یک اپلیکیشن پیام‌رسان قابل اعتماد و دارای قابلیت رمزگذاری سرتاسری دانلود کنید.

استفاده از چنین اپلیکیشن پیام‌رسانی بهترین راه برای به حداقل رساندن این خطر است که شخص سومی بتواند بر مکاتبات شما نظارت کند یا جلوی فرستادن ویدیوها یا پیام‌های شما به دیگران را بگیرد

بهترین گزینه برای شما...

«سیگنال» قابل اعتمادترین گزینه برای حفظ امنیت ارتباطات شماست، و ما به‌شدت توصیه می‌کنیم این اپلیکیشن را دانلود کنید و برای پیام‌رسانی روزمره خود استفاده کنید. کار با این اپلیکیشن بسیار ساده است، اکثر متخصصان امنیت دیجیتال آن را تایید می‌کنند و همچنین اپلیکیشن منتخب افشاگر آمریکایی، ادوارد اسنودن است.

برای دانستن جزئیات بیشتر درباره این اپلیکیشن و نحوه‌ی دانلود آن، روی لینک زیر کلیک کنید.

Signal

Android | iOS | Windows | Linux

«سیگنال» اپلیکیشن پیام‌رسانی با قابلیت رمزگذاری سرتاسری E۲EE است که از سیستم‌عامل‌های iOS، اندروید، ویندوز و لینوکس پشتیبانی می‌کند. این اپلیکیشن رایگان بوده و به عنوان یکی از ایمن‌ترین اپلیکیشن‌های پیام‌رسان موجود از سوی موسساتی چون Electronic Frontier Foundation و Access Now توصیه می‌شود.

این اپلیکیشن به کاربران خود اجازه می‌دهد تا پیام‌های ویدیویی، صوتی، نوشتاری و عکس را به صورت گروهی و رمزگذاری شده ارسال کنند. همچنین امکان تماس‌های تلفنی با قابلیت رمزگذاری سرتاسری برای کاربران «سیگنال» وجود دارد.

سهولت استفاده

شما می‌توانید «سیگنال» را برای سیستم‌های اندروید و iOS با استفاده از لینک‌های بالا بلافاصله دانلود کنید. کار با این اپلیکیشن بسیار ساده است. وقتی اپلیکیشن را باز می‌کنید، از شما خواسته می‌شود تا شماره تلفن خود را از طریق یک کد شش رقمی تایید کنید، که این کد با اس‌ام‌اس برای شما ارسال می‌شود.

وقتی این کار را انجام دادید، بلافاصله می‌توانید مکاتبات خود را با هر کدام از کانتکت‌های خود - به شرط آن‌ها هم اپلیکیشن سیگنال را دانلود کرده باشند- شروع کنید.

از اردیبهشت ۱۴۰۱ قابلیت جدیدی به سیگنال اضافه شده است که در صورت تغییر سیم کارت نیازی به اجرای دوباره برنامه نیست و اپلیکیشن شمابا همان اطلاعات قبلی و تنها با شماره جدید قابل استفاده است.

مزایا و ویژگی‌ها

سیستم رمزگذاری «سیگنال» بسیار مطمئن است، این اپلیکیشن، منتخب ادوارد اسنودن است.

سیگنال فقط پیام‌های شما را رمزگذاری نمی‌کند، بلکه فراداده‌ها را نیز پنهان می‌کند تا اطمینان حاصل شود که هیچ‌کس، نه حتی خود سیگنال یا هرکس که سعی کند تا جلوی پیام‌های شما را بگیرد، نتواند فرستنده و گیرنده پیام‌ها را شناسایی کند.

همچنین سیگنال یک اپلیکیشن متن‌باز است، این بدین معنی است که کد آن برای مشاهده همگان و کسانی که تلاش کنند آن را بشکنند، در دسترس است. تا به امروز پروتکل رمزگذاری سیگنال هرگز شکسته نشده است.

سیگنال داده‌های شما یا هیچ‌کس دیگری را جمع‌آوری نمی‌کند و به اشتراک نمی‌گذارد.

همچنین این اپلیکیشن از تیر ماه ۱۴۰۰ به بعد، از پروکسی‌های مخصوص به خود پشتیبانی می‌کند. برای دستیابی به این پروکسی‌ها می‌توانید هشتگ #IRanASignalProxy را در توئیتر دنبال کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

«سیگنال» از شماره تلفن شما برای ثبت‌نام و همینطور به عنوان شناسه‌ی شما استفاده می‌کند. به همین دلیل باید مواظب باشید که از این اپلیکیشن تنها برای برقراری ارتباط با کانتکت‌های قابل اعتماد خود استفاده کنید.

اگر تصمیم می‌گیرید که از «سیگنال» به عنوان اپلیکیشن پیش‌فرض برای فرستادن پیامک استفاده کنید، یادتان باشد که پیام‌های شما تنها در صورتی رمزگذاری می‌شوند که گیرنده نیز اپلیکیشن سیگنال را روی تلفن همراه خود نصب کرده باشد.

مورد دیگر اینکه، «سیگنال» تنها در صورت دسترسی به اینترنت به کار می‌آید. هر چند که ابزاری عالی برای استفاده روزمره است، در صورت قطع شدن اینترنت خیلی کارایی نخواهد داشت.

Session

Android | iOS | Windows | Linux

سِشِن (Session) یک پیام رسان امن با قابلیت رمزگذاری سرتاسری است که به کاربران خود اجازه می‌دهد پیام‌های ویدیویی، صوتی، نوشتاری و عکس را به صورت گروهی و رمزگذاری شده ارسال کنند. حفظ حریم خصوصی کاربر در طراحی این اپلیکیشن جایگاه ویژه‌ای داسته است؛ این برنامه برای ثبت نام نیازی به شماره تلفن ندارد و هیچ داده و یا فراداده‌ای را در خود نگه نمی‌دارد. اپلیکیش سشن که از جدیدتری پیام‌رسان‌های موجود است، کاملا رایگان و متن باز است که این باعث بررسی عمومی و رفع نقص مداوم در آن می‌شود. این برنامه مبتنی بر کلید عمومی است و از سرورهای غیر متمرکز استفاده می‌کند.

سهولت استفاده

همانطور که گفته شد این اپلیکیش برای ایجاد حساب کاربری نیازی به شماره تلفن همراه ندارد. همچنین احراز هویت و شناسایی فرد صاحب حساب در این اپلیکیشن ضروری نیست و نام کاربری شما می‌تواند هر نامی اعم از واقعی یا مستعار باشد. پس از نصب، این برنامه یک کد دراختیار شما خواهد گذاشت. برای اضافه کردن دیگران به لیست مخاطبان خود کافی است این کد را در اختیار آن‌ها قرار دهید.

مزایا و ویژگی‌ها

در این پیام‌رسان شما می‌توانید یک حساب کاربری را در چند دستگاه مختلف همگام‌سازی کنید. همچنین این امکان وجود دارد که با رمز اولیه که برنامه در هنگام نصب در اختیار شما میگذارد پس از پاک شدن احتمالی، حساب خود را بازیابی کنید. هیچ ابرداده‌ای از جمله نوع دستگاه و یا IP شما در این برنامه جمع‌آوری نمی‌شود بنابراین و اساسا داده‌هایی از این دست برای رصد کردن احتمالی وجود ندارد. از طرفی با رعایت پروتکل رمزگذاری سرتاسری، ناشناس ماندن فرستنده و گیرنده در در این برنامه لحاظ شده است. سشن از شفافیت کافی برخوردار است و سیستم کد گذاری آن برای حساب‌رسی در اختیار عموم قرار گرفته است. سشن به شما امکان داشتن گروه‌های عمومی تا حداکثر بیست نفر را می‌دهد و همزمان می‌توانید گروه‌های خصوصی‌تری از دوستان نزدیک را هم در این برنامه ساماندهی کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

با اینکه سشن یک ابزار امن و قدرتمند برای برقراری ارتباط است، اما به نظر نمی‌رسد که در حال حاضر برای مصرف کننده‌های عمومی مناسب باشد و بیشتر قابل استفاده برای افرادی است که بتوانند برخی پیچیدگی‌های کار با آن را مدیریت کنند.

امکان برقراری تماس صوتی و ویدیویی در این برنامه وجود ندارد و حداکثر حجم تبادل فایل در آن ۱۰ مگابایت است.

از معایب این برنامه می‌توان نداشتن گزینه‌ی تائید دو مرحله‌ای است را بر شمرد. همچنین و به نسبت اپلیکیشن‌هایی از این دست امکان شخصی سازی محیط در آن بسیار محدود است.

Nahoft

Android

«نهفت» که در فارسی به معنی پنهان است، یک نرم‌افزار آفلاین رمزنگاری پیام و حفظ حریم‌خصوصی برای استفاده در شبکه‌های ناامن است. در واقع «نهفت» یک پیام‌رسان نیست اما با رمزنگاری پیام‌ها، دسترسی دیگران به محتوای رد و بدل شده توسط شما و دوستان‌تان در دیگر پیام‌رسان‌ها را غیر ممکن می‌کند.
این برنامه توسط گروه حقوق بشری اتحاد برای ایران و در قالب پروژه‌ی ایران کوباتور ۲ توسعه داده شده است. سازمان اتحاد برای ایران یک نهاد حقوق بشری است که مرکز آن در شهر برکلی، ایالت کالیفرنیا قرار دارد. هدف این نهاد گسترش آزادی‌های مدنی در ایران، دفاع از حقوق بشر، حمایت از جامعه مدنی و ترغیب به مشارکت از طریق فناوری است.

سهولت استفاده

این نرم افزار متن باز که با تکنیک پنهان‌نگاری (Steganography) طراحی شده، کاملا آفلاین است و از هیچ سروری جهت ارسال یا دریافت یا رمزگذاری پیام‌های شما استفاده نمی‌کند.
شما می‌توانید متن خود را رمزگذاری کنید و آن را از طریق متن، کلمات شانسی یا انتخاب یک تصویر از گالری دستگاه خودتان ارسال کنید.
شما همچنین می‌توانید یک پیام را رمزگذاری کنید، آنرا در یک تصویر بگنجانید و در حافظه دستگاه خود نگهداری کنید.
در عین حال این امکان وجود دارد که پس از رمزگشایی و خواندن پیام دریافتی آن را در نهفت ذخیره کنید و یا در همان لحظه آن را پاک کنید.
همچنین این برنامه دارای قابلیت تعریف یک کد ورود تخریبی است. ایجاد این کد به شما کمک میکند که در زمان اضطرار و هنگامی که احتمال دسترسی دیگران به گوشی تلفن همراه شما ممکن است از آن استفاده کرده و تمام اطلاعات ذخیره شده در این نرم افزار را در یک لحظه پاک کنید.
نهفت در دو مرحله توسط پژوهشگران و متخصصان Cure۵۳ ارزیابی امنیتی شده و پیش از انتشار آخرین نسخه، پیشنهادات آنان برای بهبود امنیت اپ به کار گرفته شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از آنجایی که اصولا فرآیند رمزنگاری فرآیند پیچیده‌ای است ممکن است استفاده از این برنامه برای تمام کاربران ساده نباشد. همچنین برخی کاربران از پیچیده بودن رابط کاربری این برنامه گلایه کرده‌اند.
این برنامه تا کنون تنها برای سیستم عامل اندروید طراحی شده و نسخه‌ای برای اپل، ویندوز و لینوکس ارائه نکرده است.

دانلود این اپلیکیشن‌ها را نیز برای استفاده در آینده در نظر بگیرید.

دو اپلیکیشن «برایر» و «جمی»، پیام‌رسان‌هایی با رمزگذاری سرتاسری هستند که بر اساس فناوری‌های همتا به همتا (peer-to-peer) ساخته شده‌اند و اگر پیش‌بینی می‌کنید که ممکن است با مشکلات اتصال به اینترنت (از قطع شدن اینترنت گرفته تا مثلاً وای‌فای ضعیف در یک کنفرانس پرجمعیت) روبه‌رو باشید، گزینه‌های خوبی هستند.
البته احتمالا کار کردن با «سیگنال» برای استفاده روزمره و ارتباط با دوستان و خانواده، راحت‌تر خواهد بود. می‌توانید درباره‌ی این اپلیکیشن‌ها در لینک‌های زیر بیشتر بخوانید.

Jami

Android | iOS | Windows | Linux

«جمی» پلتفرم رایگان برای ارتباط و مکاتبه است که ادعا می‌کند هویت و حریم خصوصی کاربران خود را حفاظت می‌کند. «جمی» دارای رمزگذاری سرتاسری است و به شکل همتا به همتا عمل می‌کند، بنابراین نیازی به یک سرور مرکزی برای انتقال داده بین کاربران ندارد.
به همین سبب، کاربرانی که روی یک شبکه‌ی محلی مشترک هستند (برای مثال، یک شبکه وای‌فای عمومی بدون دسترسی به اینترنت) باید بتوانند از طریق «جمی» به هم متصل شوند، حتی اگر به اینترنت وصل نباشند.

سهولت استفاده

دانلود این اپلیکیشن برای اندروید از گوگل‌پلی، و برای iOS از اپل استور امکانپذیر است. نسخه‌های مخصوص دسکتاپ (مک، ویندوز و لینوکس) را هم می‌توان از خود وبسایت «جمی» دانلود کرد.
برای ایجاد حساب جمی نیازی به ارائه هیچ مشخصات فردی و یا حتی شماره تلفن نیست.

مزایا و ویژگی‌ها

علاوه بر برقراری ارتباط امن، «جمی» تماس‌های ویدویی و کنفرانسی با کیفیت اچ‌دی را نیز ارائه می‌کند، اما کیفیت این تماس‌ها بسیار بستگی به کیفیت اینترنت مورد استفاده دارد.
داشتن قابلیت ارسال پیام از طریق شبکه‌های وای‌فای می‌تواند در زمان‌های قطع موقت اینترنت (و حتی قطع کامل اینترنت) به منظور برقراری ارتباط با کانتکت‌هایی که در نزدیکی شما هستند، موثر عمل کند. «جمی» همچنین ممکن است بتواند در صورت محدود شدن دسترسی به اینترنت جهانی به شکلی مطمئن عمل کند، اما تنها در صورتی که اینترنت ملی در دسترس باقی بماند.
به این موضوع توجه داشته باشید که محققان ما به صورت مستقل قادر به تایید این گزارش‌ها نبوده‌اند، بنابراین نمی‌توانند درباره کارکرد این اپلیکیشن در چنین شرایطی با قطعیت نظر بدهند. آزمایش‌ها و شواهد بیشتری برای این کار نیاز است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

بر خلاف برخی از اپلیکیشن‌هایی که بر پایه‌ی شبکه توری meshnet-based طراحی می‌شوند، «جمی» قادر به استفاده از بلوتوث برای برقراری ارتباط با دستگاه‌های دیگر نیست. برقراری ارتباط آفلاین با کانتکت‌ها، نیازمند اتصال هر دو طرف به یک شبکه‌ی اینترنت مشترک محلی است.
همچنین سازندگان راهی برای درخواست از بین بردن کامل اطلاعات در این اپلیکیشن در نظر نگرفته‌اند.

Briar

Android | F-Droid app

«برایر» یک اپلیکیشن پیام‌رسان است که برای استفاده کنشگران، روزنامه‌نگاران و هر کس دیگری که احتیاج به برقراری ارتباط در زمان قطع اینترنت داشته باشد، طراحی شده است. برخلاف اپلیکیشن‌های پیام‌رسان سنتی، «برایر» متکی بر یک سرور مرکزی نیست، پیام‌ها با استفاده از یک شبکه توری به صورت مستقیم بین دستگاه‌های کاربران همزمان‌سازی یا همان synchronized می‌شوند.

سهولت استفاده

کاربران می‌توانند «برایر» را برای اندروید از پلی استور گوگل، F-Droid یا وب سایت برایر دانلود نمایند..

مزایا و ویژگی‌ها

«برایر» می‌تواند برای به اشتراک گذاشتن پیام‌های مهم با افرادی که به آن‌ها اعتماد دارید، به شکلی مطمئن عمل کند. در هنگام قطع شدن اینترنت، این اپلیکیشن اجازه می‌دهد تا داده‌ها و اطلاعات را با لیست مخاطبان(کانتکت‌ها) خود به شکلی امن به اشتراک بگذارید، البته لازم خواهید داشت تا با فرد گیرنده در محدوده‌ی بلوتوث یا روی یک شبکه وای‌فای مشترک قرار داشته باشید.

علاوه بر قابلیت گپ زدن سرتاسری خصوصی و گروهی، «برایر» به شما این امکان را می‌دهد تا تالارهای گفتگوی عمومی و بلاگ‌هایی تشکیل دهید که برقراری ارتباط را با گروه‌های معتمد میسر می‌سازد، و حتی در زمان‌های قطع اینترنت هم قابل اشتراک‌گذاری و به‌روزرسانی هستند.

تالارهای گفتگو، مکالمات غیر خصوصی هستند. بر خلاف گروه‌های خصوصی، هر کسی که به آن بپیوندد می‌تواند کانتکت‌های دیگر خود را به تالار دعوت کند. در ضمن بلاگ‌ها امکان پست و به اشتراک گذاشتن اخبار و بروزرسانی‌ها را با تمام کانتکت‌هایتان امکان پذیر می‌سازند.

«برایر» همچنین با اپلیکیشن "دکمه هشدار" Ripple مجهز شده است که می‌تواند برایر را مخفی کند یا در حالتی که نگران هستید حساب کاربری شما تحت نظارت قرار گرفته یا مصادره شده، می‌تواند طوری پیکربندی شود که حساب کاربری و تاریخچه پیغام‌های شما را پاک کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

این اپلیکیشن البته اشکالاتی نیز دارد. گزارش‌هایی از مشکلات برقراری ارتباط از طریق بلوتوث در زمانی که اینترنت قطع شده است دریافت شده، اما گروه «برایر» مشغول رفع این اشکالات هستند.

در زمان قطع اینترنت، این اپلیکیشن تنها در صورتی که کاربران در محدوده بلوتوث و وای‌فای یکدیگر قرار داشته باشند، می‌تواند کارایی داشته باشد.

مشکل دیگر این اپلیکیشن این است که تا زمانی که تعداد زیادی از افراد شروع به استفاده از «برایر» نکنند، نمی‌تواند در زمان‌های قطع دسترسی به اینترنت از تمام امکانات بالقوه خود استفاده کند و موثر واقع شود. برای اینکه «برایر» بتواند به یک اپلیکیشن پیام‌رسان قدرتمند تبدیل شود و جایگزین پیام‌رسان‌های معمول بشود، می‌بایست تعداد کاربران گسترده‌ای را جذب کند.

ابزار دور زدن

هر کسی که خواسته به وب‌سایت‌های فیلتر شده روی اینترنت جهانی دسترسی پیدا کند، به این سوال برخورد کرده است که کدام وی‌پی‌ان را باید انتخاب کرد. این‌ها ابزارهایی هستند که برای دسترسی به محتوای فیلترشده بکار شما می‌آیند و همچنین اتصال شما را رمزگذاری می‌کنند تا در برابر ناظران بیرونی امنیت داشته باشید.
دوستان ما در «پس‌کوچه»، فهرست بسیار خوبی از ابزارهای دور زدن فیلترینگ را به همراه مروری دقیق و کامل بر مزایا و معایب این ابزارها جمع‌آوری کرده‌اند. اگر آنچه به دنبالش هستید را در فهرست منتخب ما پیدا نکردید، «پس‌کوچه» می‌تواند اطلاعات بیشتری درباره ابزارهای دور زدن موجود به شما ارائه دهد.
تشخیص تیم ما بر این بوده است که نمونه‌های ذیل از موثرترین و قابل اعتمادترین ابزارها برای دور زدن سانسور معمول و هر روزه هستند. همه‌ی مواردی که اینجا جمع‌آوری کرده‌ایم به عنوان ابزارهای حفظ هویت و حریم خصوصی طراحی نشده‌اند، پس حتماً توضیحات هر کدام را بخوانید و متوجه تفاوت‌های بین این ابزارها باشید تا بتوانید امنیت آنلاین خود را حفظ کنید.

Psiphon

Android | iOS | Windows | Android direct source

««سایفون» ابزاری برای دور زدن فیلترینگ است که از فناوری‌های وی‌پی‌ان، اس‌اس‌اچ و اچ‌تی‌تی‌پی استفاده می‌کند تا دسترسی بدون سانسور به محتوای اینترنت را برای شما فراهم کند. این اپلیکیشن به صورت خودکار به نقاط دسترسی جدید پی می‌برد تا احتمال دور زدن فیلترها را برای شما بالا ببرد.

سهولت استفاده

کار کردن با «سایفون» خیلی راحت است. فقط لازم است آن را از طریق یکی از لینک‌های بالا روی دستگاه خود دانلود و نصب کنید. بعد از اینکه نصب شد، اپلیکیشن را باز کنید و روی 'connect' بزنید تا «سایفون» روی دستگاه فعال شود..

مزایا و ویژگی‌ها

«سایفون» سابقه‌ی طولانی در دور زدن سانسور اینترنتی در ایران دارد و همچنان برای این منظور کارایی خود را حفظ کرده است.

هر چند در زمان‌های وقوع اختلال در اینترنت و یا قطع کامل از کارایی آن کم می‌شود، بخش کوچکی از کاربران «سایفون» گزارش داده‌اند که طی قطع شدن اینترنت در آبان ۱۳۹۸ به محتوای اینترنت جهانی دسترسی داشته‌اند. تحقیقات مکملی که از سوی«سایفون» صورت گرفت نیز صحت این موضوع را تایید کرد.

در نسخه‌ی ۵.۰ و بالاتر اندروید فیلترشکن سایفون، امکان غیر فعال کردن برنامه‌هایی که نمی‌خواهید از تونل سایفون رد شوند را دارید.

بدین ترتیب می‌توانید از این فیلتر شکن هدفمندتر استفاده کرده و در مصرف حجم اینترنت نیز صرفه جویی کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

باگر دنبال دست یافتن به اطلاعات حساس یا به اشتراک گذاشتن آن هستید، نباید فقط به این اپلیکیشن متکی باشید.

هرچند که با استفاده از «سایفون»، ISP شما قادر به دیدن محتوای در حال داد و ستد شما نخواهد بود، اما این اپلیکیشن مانع این نمی‌شود که تاریخچه مرورگر و کوکی‌ها بر روی دستگاه شما ذخیره نشوند.

توجه داشته باشید که «سایفون» برخی اطلاعات در رابطه با ناحیه، کشور و فعالیت‌های انجام شده روی مرورگر شما و زمان و تاریخ آن ها را ثبت می‌کند. برنامه‌نویسان «سایفون» این داده‌ها را جمع‌آوری و تحلیل کرده و سپس آن‌ها را حذف می‌کنند. خط مشی «سایفون» در رابطه با حفظ حریم خصوصی به زبان فارسی در اینجا موجود است، که در مورد جمع‌آوری داده‌ها و نحوه‌ی به اشتراک گذاشتن آن‌ها با طرف ثالث در آن توضیح داده شده است.

Lantern 

Android| iOS | Windows | GitHub

«لنترن» یک نوع اپلیکیشن دور زدن فیلترینگ است که چندین روش مختلف را برای گذر از فیلتر و سانسور بکار می‌گیرد و بسته به تغییراتی که سانسورچی ایجاد می‌کند، از روشی به روش دیگر می‌رود. این ابزار، فیلتر بودن یا نبودن یک وب‌سایت را تشخیص می‌دهد و تنها در این صورت که وبسایت خارج از دسترس باشد، شروع به استفاده از شیوه‌های دور زدن می‌کند. این امر به این معناست که می‌تواند به وب‌سایت‌های فیلتر نشده سریع‌تر متصل شود.
هر چند اکثر مواقع سرعت بالایی ارائه می‌دهد و داد و ستد داده‌های شما را در وب‌سایت‌های فیلتر شده رمزگذاری می‌کند، اما ادعا نمی‌کند که از هویت کاربران خود حفاظت می‌کند و امکان این را ندارد که کاربران را در برابر نظارت و شنود، مانند اپلیکیشن‌های دیگری مثلاً «تور» Tor، محافظت کند.

سهولت استفاده

کار با «لنترن» نسبتاً سرراست است. فقط لازم است که با استفاده از یکی از لینک‌های بالا روی دستگاه خود دانلود و نصبش کنید. بعد از اینکه نصب شد، اپلیکیشن را باز کنید و connect را بزنید تا فعال شود.

مزایا و ویژگی‌ها

ویژگی اصلی «لنترن» این است که دسترسی به وب‌سایت‌های فیلتر شده را با سرعت بالایی ارائه می‌دهد. در شرایط معمول ایران، این اپلیکیشن معمولاً ثابت کرده که در شکستن فیلترهای حکومتی موثر عمل می‌کند.
به همین دلیل برای استفاده روزمره کاربران معمولی و گذر از فیلترینگ دولتی ایران، مناسب‌ترین ابزار است، اما برای استفاده روزنامه‌نگاران و کنش‌گرانی که فاش نشدن هویت خودشان را باید در اولویت قرار دهند، ابزار مناسبی نیست. اگر حفظ کامل حریم خصوصی و هویت، برای شما موضوع مهمی است، باید به دنبال وی‌پی‌انی باشید که مخصوصاً برای این منظور طراحی شده باشد.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

در آبان ۱۳۹۸ که اینترنت ایران قطع شده بود، «لنترن» آنچنان که باید موثر عمل نکرد و هیچ گزارش موثقی مبنی براینکه کاربران «لنترن» بعد از قطع شدن اینترنت توانسته باشند به اینترنت جهانی وصل شوند، دریافت نشده است. به همین دلیل ما کار با این اپلیکیشن را فقط در وضعیت«عادی» توصیه می‌کنیم.
همانطور که گفته شد، «لنترن» هیچ ادعایی مبنی بر اینکه هویت شما را محفوظ نگه می‌دارد، نداشته است. هر نوع ارتباطی که از طریق «لنترن» ایجاد شده باشد، رمزگذاری می‌شود اما این نرم‌افزار نمی‌تواند هیچ اقدامی در جهت محافظت کاربران در برابر وبسایت‌هایی که کاربران خود را رصد می‌کنند یا در برابر نظارت و شنود حکومتی، انجام دهد.
«لنترن» اطلاعات شخصی مربوط به ناحیه، کشور و فعالیت‌های انجام شده روی مرورگر شما و زمان و تاریخ آن ها را ثبت می‌کند. این داده‌ها پیش از آن که از طرف برنامه‌نویسان این نرم‌افزار تحلیل شوند، جمع‌آوری aggregate می‌شوند و تنها در حالتی با طرف ثالث به اشتراک گذاشته می‌شوند که کاملا aggregate و گمنام‌سازی شده باشند.
اطلاعات بیشتر در بخش «خط مشی در زمینه حریم خصوصی» لنترن در اینجا به زبان انگلیسی موجود است.

Proton VPN

Android | iOS | Windows | Linux

«پروتون وی‌پی‌ان» یک رساننده خدمات شبکه مجازی خصوصی است که با پشتوانه مالی جمعی حمایت می‌شود و از سوی بنیانگذاران خدمات امنیت ایمیل «پروتون میل» عرضه شده است. این اپلیکیشن محافظت از امنیت و حریم خصوصی کاربران را در سطح بسیار بالایی تامین می‌کند.
نکته‌ی بسیار مهم این است که «پروتون وی‌پی‌ان» نسخه‌ی رایگانی از خدمات خود را بدون هیچ محدودیت در ترافیک داده، به کاربران این رده ارایه می‌دهد.
این وی‌پی‌ان که ۱۷۰۰ سرور در ۶۰ کشور جهان دارد با نرخ انتقال داده‌ی ۶۰ مگابایت بر ثانیه از سرعت قابل قبولی نیز برخوردار است هر چند نمیتوان مطمئن بود که شما در نسخه رایگان نیز از همین سرعت برخوردار باشید.

سهولت استفاده

روند ثبت‌نام بسیار سرراست است. اگر از وی‌پی‌ان دیگری دارید استفاده می‌کنید، به وبسایت «پروتون وی‌پی‌ان» بروید و با ایمیل خود یک حساب کاربری باز کنید، سپس نام کاربری و کلمه‌ی عبور خود را انتخاب کنید. بعد از آن دیگر می‌توانید نسخه‌ی مناسب دستگاه خود را دانلود کنید.

مزایا و ویژگی‌ها

روش کار «پروتون وی‌پی‌ان» بر این اساس است که هیچ داده‌ای را ثبت نکند، و خط مشی مکتوب بسیار دقیق و واضحی دارد که می‌توانید آن را به زبان انگلیسی در اینجا بخوانید. این اپلیکیشن طوری طراحی شده که یک تونل رمزگذاری شده بین شما و سرورهای خود ایجاد می‌کند، و با این کار از شما در برابر نظارت و شنود دشمنان محافظت کرده و تاریخچه فعالیت‌های شما را از آی‌اس‌پی مخفی نگه می‌دارد.
اپلیکیشن‌های «پروتون وی‌پی‌ان» روی همه‌ی پلتفرم‌ها کاملاً متن‌باز هستند و امنیت آن‌ها به صورت مستقل بررسی دقیق شده است. این وی‌پی‌ان همچنین دارای قابلیت قطع اضطراری (kill switch) است که در صورت قطع شدن وی‌پی‌ان، جلوی ترافیک اینترنت را بر روی دستگاه شما می‌گیرد. این موضوع باعث می‌شود که تصادفا بدون محافظت نمانید.
سرورهای «پروتون وی‌پی‌ان» در سوئیس مستقر هستند، کشوری که قوانین سفت و سختی در زمینه‌ی حفاظت از حریم خصوصی دارد و سابقه نشان داده که در برنامه‌های اشتراک‌گذاری اطلاعات و جاسوسی بین‌المللی وارد نمی‌شود.
بر اساس این قوانین و ویژگی‌ها، می‌توان گفت که «پروتون وی‌پی‌ان» دارای کارنامه‌ای قوی در زمینه‌ی حریم خصوصی، امنیت و رمزگذاری است و اگر به دنبال وی‌پی‌ان رایگان هستید می‌تواند انتخاب خوبی باشد..

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

برای استفاده از «پروتون وی‌پی‌ان» لازم است که حتما در آن ثبت‌نام کنید که این موضوع ممکن است چالش‌هایی را در مواقع اختلال اینترنت یا وقتی که وب‌سایت اپلیکیشن فیلتر شده باشد، به وجود آورد. توصیه می‌شود که برای ثبت‌نام از آدرس ایمیلی غیر از آدرس همیشگی خود استفاده کنید.
همانند دیگر وی‌پی‌ان‌های تجاری، بسته‌ی رایگان «پروتون وی‌پی‌ان» به احتمال زیاد نسبت به نسخه‌های پولی آن، تأثیرات منفی زیادی روی سرعت اینترنت شما خواهد داشت. هر چند این اپلیکیشن ابزاری مهم و کارآمد برای حفاظت از هویت شما و گذر از فیلترها است، این موضوع می‌تواند به قیمت پایین آمدن سرعت اینترنت تمام می‌شود.

TunnelBear

Android| iOS| Windows

«تونل بر» سرویس وی‌پی‌انی است که می‌توانید برای گشت و گذار در اینترنت به شکل محرمانه و امن استفاده کنید. وی‌پی‌ان مطمئن«تونل بر»حریم خصوصی آنلاین شما را حفظ کرده و از طریق استفاده از یک شبکه‌ی خصوصی مجازی(Virtual Private Network – VPN) موقعیت مکانی شما را از دسترس خارج می‌کند. در این روش، اطلاعات به صورت رمزگذاری‌شده به سرور وی‌پی‌ان منتقل می‌شوند و از آن جا به سایت مقصد می‌رسد.نکته‌ی مهم این است که «تونل بر» دارای بسته‌ی رایگانی برای کاربران ایرانی است. این بسته شامل ۱۰ گیگابایت سرویس رایگان در ماه برای کاربران درون ایران است. این اپلیکیشن از چند حسابرسی امنیتی مستقل سربلند بیرون آمده و بنابراین باید بتواند در حفظ امنیت و حریم خصوصی شما در فضای آنلاین موثر واقع شود.

سهولت استفاده

اپلیکیشن «تونل بر» را می‌توانید با استفاده از یکی لینک‌های بالا، مناسب با نوع سیستم‌عامل خود دانلود کنید.
پس از اینکه اپلیکیشن را باز کردید، لازم است که با ایمیل خود یک حساب کاربری بسازید (ما توصیه می‌کنیم از آدرس ایمیل همیشگی خود استفاده نکنید). پس از آن می‌توانید به وی‌پی‌ان متصل شوید.

مزایا و ویژگی‌ها

«تونل بر» بر اساس این سیاست عمل می‌کند که هیچ داده‌ای ثبت نشود، به این معنی که داده‌های مرتبط با آدرس IP شما و یا وب‌سایت‌هایی را که بازدید می‌کنید، ذخیره نمی‌کند. خط مشی مربوط به حریم خصوصی این اپلیکیشن را می‌توانید به زبان انگلیسی دراینجا خوانید که جزییات جامعی درباره‌ی شیوه‌های جمع‌آوری داده به شکل محدود و بدون افشای هویت در آن ارائه شده است.
همانطور که اشاره شد، این اپلیکیشن از چندین حسابرسی امنیتی مستقل سربلند بیرون آمده و بر همین اساس می‌توانیم بگوییم که ابزاری معتبر است و قابلیت‌های آن در زمینه حفظ هویت و حریم خصوصی و همینطور دور زدن فیلترینگ ثابت شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

«تونل بر» در حال حاضر در بسته‌ی رایگان خود تا سقف ۵۰۰ مگابایت در ماه محدودیت استفاده دارد. این موضوع به این معنی است که نباید برای دسترسی به محتوای سنگین مثل تعداد زیاد عکس و فیلم، به این اپلیکیشن متکی بود.
همچنین این سرویس از شما می‌خواهد تا با ایمیل خود در آن ثبت‌نام کنید که می‌تواند در زمان اختلال و قطع شدن اینترنت و یا فیلترینگ، مشکل‌زا شود. علاوه بر این، به شما توصیه می‌شود که از آدرس ایمیل همیشگی خود برای ثبت‌نام استفاده نکنید.

Windscribe VPN

Android | iOS | Windows | Linux

«ویندسکرایب» یک سرویس وی‌پی‌ان تجاری است که می‌توانید برای گشت و گذار آزادانه و امن در اینترنت از آن استفاده کنید. از حریم خصوصی شما محافظت می‌کند و به شما کمک می‌کند تا فیلترهای اینترنتی را دور بزنید.
بسته‌ی رایگان «ویندسکرایب» در هر ماه ۱۰ گیگابایت ترافیک داده ارائه می‌دهد که بسیار دست و دلبازانه است.
همچنین فایروال «ویندسکرایب» روی این بسته موجود است که ادعا می‌کند تمام اتصالات را خارج از تونل خودش می‌بندد تا هیچ داده‌ای از ارتباط شما به بیرون درز نکند.

سهولت استفاده

این اپلیکیشن را از یکی از لینک‌های بالا دانلود کنید. وقتی برای اولین بار اپلیکیشن را باز می‌کنید، از شما خواسته می‌شود تا یک حساب کاربری بسازید. یک آدرس ایمیل و کلمه‌ی عبور انتخاب کنید (ترجیحا آدرس اصلی شما نباشد)، حالا این فرصت را دارید تا ۱۰ گیگابایت ترافیک ماهانه رایگان خود را طلب کنید.
بعد از اینکه این کار را انجام دادید، می‌توانید وی‌پی‌ان را روی دستگاه خود فعال کنید.

مزایا و ویژگی‌ها

هر چند که سرعت این اپلیکیشن ممکن است همیشه به خوبی وی‌پی‌ان‌های دیگر نباشد، اما نشان داده که در ایجاد دسترسی کاربران ایرانی به محتوای فیلترشده بسیار موثر عمل می‌کند.
فایروال موجود در این اپلیکیشن نیز یک لایه‌ی محافظت دیگر به حریم خصوصی اضافه می‌کند تا از خطر نشت اطلاعات از تونل وی‌پی‌ان شما جلوگیری کند.
این اپلیکیشن قابلیت تقسیم تونل را دارد که به شما امکان می‌دهد به طور خاص انتخاب کنید کدام برنامه‌ها از وی‌پی‌ان استفاده کنند. این به معنی صرفه‌جویی قابل توجه در مصرف اینترنت شماست.
از مزایای دیگر این وی‌پی‌ان امکان انتخاب میان چهار پروتکل OpenVPN UDP/TCP, IKEv۲, Stealth است که به سرعت و امنیت وبگردی شما کمک میکند

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

همچون دیگر وی‌پی‌ان‌های تجاری، «ویندسکرایب» نیز به احتمال زیاد در صورت قطع شدن مستمر اینترنت، اختلال در آن و یا پایین آمدن سرعت، خیلی خوب کار نخواهد کرد.
هرچند که می‌تواند ابزار بسیار مفیدی برای رد شدن از فیلترها باشد، اما باید توجه داشته باشیم که به اندازه‌ی ابزارهای دور زدن برگرفته از Tor ، در حفظ هویت شما موثر عمل نخواهد کرد.

1.1.1.1 + WARP

Android | iOS | Windows | LINUX

اپلیکیشن ۱.۱.۱.۱ شرکت Cloud-flare یک برطرف‌کننده‌ی دی‌ان‌اس است که تقریباً شبیه وی‌پی‌ان عمل می کند. ترافیک اینترنت شما را از یک تونل مطمئن رد کرده، رمزگذاری کرده و ادعا می‌کند که داده‌های مرورگر شما را به طرف ثالث نشان نمی‌دهد.
هر چند که احتمالا از نظارت ISP شما بر وب‌سایت‌هایی که باز می‌کنید جلوگیری می‌کند، اما باعث نمی‌شود که اتصال شما به وب‌سایت‌ها بدون فاش شدن هویت شما اتفاق بیفتد، و همچنین قادر نیست سانسورها را به خوبی وی‌پی‌ان دور بزند. البته می‌تواند در حد ابتدایی امنیت فضای آنلاین شما را فراهم کند و در عین حال سرعت قابل قبولی داشته باشد، اما این اپلیکیشن به اندازه‌ی وی‌پی‌ان‌هایی که مخصوص امنیت حریم خصوصی ساخته شده‌اند، موثر نخواهد بود.

سهولت استفاده

شما می‌توانید ۱.۱.۱.۱ + WARP را از گوگل پلی، اپ‌استور یا پس‌کوچه دانلود کنید. وقتی که اپلیکیشن را نصب و باز کردید، دستورالعمل را دنبال کنید و دکمه‌ی اسلایدر را برای اتصال روشن کنید.

مزایا و ویژگی‌ها

این اپلیکیشن رایگان است و کار با آن بسیار ساده است. نسخه‌ی پولی آن نیز موجود است که سرعت اتصال شما را تا ۳۰٪ بالاتر می‌برد.
این اپلیکیشن به دست شرکت Cloud-flare تهیه شده است، نامی معتبر در زمینه‌ی امنیت وب‌سایت و اپلیکیشن که کارنامه بسیار درخشانی در حفظ امنیت داده‌های کاربران خود دارد. این شرکت دارای سیاست «ثبت نکردن داده» است و هیچگونه اطلاعات شخصی قابل شناسایی مربوط به استفاده شما از این اپلیکیشن را ذخیره نمی‌کند.
همچنین استفاده از این اپلیکیشن سبب میشود که سرویس‌دهنده اینترنت شما نتواند داده‌های مربوط به الگوهای فعالیت شما را در اینترنت برای فروش به تبلیغ کنندگان، جمع‌آوری کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌ده

این اپلیکیشن به عنوان یک ابزار برای دور زدن طراحی نشده است، و بنابراین نباید انتظار داشت که به وب‌سایت‌های سانسور شده تحت هر شرایطی دسترسی ایجاد کند. بعضی از کاربران گزارش داده‌اند که استفاده از این اپلیکیشن برای باز کردن برخی وب‌سایت‌ها و اپلیکیشن‌ها مانند یوتیوب و گوگل پلی استور، چالش‌برانگیز بوده است.
همانطور که پیشتر اشاره شد، این اپلیکیشن تنها میزان محدودی امنیت حریم خصوصی فراهم می‌کند. هر چند که فعالیت‌های شما را از ISP مخفی نگه می‌دارد، اما IP شما را از وب‌سایت‌هایی که دیدن می‌کنید پنهان نمی‌کند.

Outline

Android| iOS| Windows| Linux

اوتلاین فرایند ساختن یک وی‌پی‌ان (VPN) را آسان‌تر و کم‌هزینه‌تر می‌کند و به شما اجازه می‌دهد تا آن را مدیریت کنید و کاربران را به سرور خودتان اضافه کنید. شما می‌توانید سرورهایی را روی آمازون، گوگل یا هر شرکت ارائه‌دهنده‌ی خدمات ابری دیگر قرار دهید. یکی از راه‌هایی که حکومت‌ها سرورهای وی‌پی‌ان را مسدود می‌کنند، از طریق تشخیص حجم بالای مصرف آنها است.
با این حال، با توجه به این‌که شما از طریق اوتلاین فقط از یک وی‌پی‌ان خصوصی برای خودتان و گروه محدودی استفاده می‌کنید، می‌تواند شناسایی‌شدن وی‌پی‌ان را بسیار دشوارتر کند.

سهولت استفاده

نرم‌افزار اوتلاین منیجر مناسب برای سیستم‌تان را نصب کنید و ارائه‌دهنده‌ی سرویس ابری خودتان را انتخاب کنید. پس از انتخاب آن، با فرایند آماده‌سازی خاص آن‌ها آشنا خواهید شد. شما می‌توانید سرورتان را از روی اوتلاین منیجر مدیریت کنید.
پس از تنظیم سرورتان، می‌توانید کلیدهای دسترسی یکتایی را مستقیماً از نرم‌افزار دسکتاپ منیجر ایجاد کنید. منیجر به شما امکان می‌دهد تا دعوت‌نامه‌هایی را از طریق پلتفرم ارتباطی دلخواه، برای اتصال به سرورتان بفرستید. کلیدهای دسترسی یعنی چگونه دستگاه‌هایتان را به اوتلاین منیجر وصل می‌کنید و با استفاده از سرورتان از آن‌ها محافظت می‌کنید. هر کلید دسترسی خاص و یکتاست و می‌تواند مستقیماً از روی سرور تنظیم یا حذف شود. محدودیت‌های داده، به شما امکان می‌دهد تا میزان پهنای باند مجاز برای هر کلید را کنترل کنید.
سپس، اپ اوتلاین کلاینت را دانلود کنید و با استفاده از کلید دسترسی خاص خودتان وصل شوید. اپ کلاینت نسخه‌هایی برای دسکتاپ و دستگاه‌های همراه دارد، بنابراین می‌توانید از هرجایی که باشید و از تمام دستگاه‌هایتان به اینترنت آزاد دسترسی پیدا کنید و به‌طور خصوصی با دیگران ارتباط برقرار کنید.

مزایا و ویژگی‌ها

از آنجا که وی‌پی‌انی که شما روی سرورتان اجرا می‌کنید فقط به وسیله‌ی شما و گروه محدودی مورد استفاده قرار می‌گیرد، شناسایی آن بسیار دشوارتر است و کارکردن با آن نیز باید خیلی ارزان‌تر باشد. اوتلاین همچنین می‌گوید که از یک «پروتکل بدون دست‌دادن و شبیه به هیچ‌چیز که شناسایی‌اش دشوار است» استفاده می‌کند، که باعث می‌شود کار مأموران حکومتی در تشخیص و مسدود کردن آن سخت‌تر شود.
در صورتی که سرور شما مسدود شود، باید به‌سادگی بتوانید یک سرور دیگر را با استفاده از همین روش از نو راه‌اندازی کنید.
این برنامه اطلاعات شخصی کاربران و اطلاعات وبسایت‌هایی که او مشاهده یا با آن‌ها ارتباط برقرار می‌کند را جمع‌آوری نمی‌کند. اطلاعاتی که این برنامه جمع‌آوری می‌کند را می‌توانید اینجا به تفصیل مطالعه کنید.
اوتلاین متن‌باز است و در دو بررسی امنیتی مستقل تایید شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

هر وی‌پی‌ان امنی به دسترسی به سرورهای بین‌المللی روی سرویس‌های ابری وابسته است و بنابراین در صورت قطعی کامل اینترنت، وی‌پی‌ان خصوصی شما کم‌وبیش قطعاً از کار خواهد افتاد، درست مانند هر وی‌پی‌ان تجاری دیگری که در بازار موجود است.

به صورت گمنام از اینترنت استفاده کنید.

بسیاری از وی‌پی‌ان‌ها قادر هستند تا میزان بالایی حریم خصوصی برای شما فراهم کنند، اما باید این نکته را لحاظ کرد که این ابزارها نمی‌توانند گمنام ماندن شما را به طور کامل تضمین کنند چرا که عوامل دولت شیوه‌هایی برای تشخیص آدرس IP شما در حین استفاده از وی‌پی‌ان، در دست دارند.
اما گزینه‌های دیگری وجود دارد و اتصال به اینترنت از طریق Tor می‌تواند میزان بالاتری از گمنامی را، نسبت به وی‌پی‌ان‌ها، برای شما فراهم کند. برای رسیدن به این هدف، Tor از روش مسیریابی پیازی 'onion routing' استفاده می‌کند، روشی که اتصال شما را پیش از رسیدن به مقصد منتخب، از چندین پروکسی (یا مسیریاب‌های پیازی) می‌گذراند.
این پروکسی‌ها فقط می‌توانند یک مرحله را در هر سمت از این زنجیره ببینند، بنابراین هیچ‌کس نمی‌تواند هم نقطه مبدأ ترافیک (یعنی شما) و هم نقطه مقصد (وب‌سایتی که باز می‌کنید) را مشاهده کند.
توجه کنید که ISP شما می‌فهمد که شما از Tor استفاده می‌کنید، اما هیچ چیز دیگری درباره فعالیت‌های آنلاین شما بدست نخواهد آورد. تمام کاربران Tor به چشم یک ناظر شبیه هم به نظر خواهند رسید.
خود این موضوع که شما از Tor استفاده می‌کنید می‌تواند موجب سوءظن شود، اما عقیده اکثریت قریب به اتفاق متخصصان امنیت دیجیتال این است که گمنامی بدست آمده از Tor مولفه‌ی مهمی از امنیت دیجیتال روزمره است، حتی اگر سرعت اتصال شما را بیشتر از وی‌پی‌ان‌ها پایین بیاورد.
اگر فقط می‌خواهید از Tor برای گشت و گذار در اینترنت استفاده کنید، می‌توانید مرورگر Tor را دانلود کنید، و اگر می‌خواهید بقیه اپلیکیشن‌ها روی گوشی همراهتان نیز از طریق شبکه‌ی Tor، پروکسی شوند، Orbot را دانلود کنید.

Tor Browser

Android | MacOS | Windows | LINUX

مرورگر «تور» یک مرورگر متن‌باز است که با هدف حفظ حریم خصوصی شما در فضای آنلاین و همچنین عبور از فیلترها طراحی شده. روش کار آن به این صورت است که ترافیک شما را پیش از رسیدن به مقصد، حداقل بین سه گره‌ی اتصالی (سرورهای داوطلب) حرکت می‌دهد.

سهولت استفاده

مرورگر «تور» روی سیستم عامل ویندوز و MacOS و همچنین گوشی‌های همراه اندروید موجود است ولی هنوز روی دستگاه‌های iOS وجود ندارد. از طریق لینک‌های بالا می‌توانید آن را دانلود و نصب کنید.

نصب کردن مرورگر «تور» تا حدی از ابزارهای دیگری که در اینجا معرفی کرده‌ایم پیچیده‌تر است. وبسایت پس‌کوچه دستورالعمل نصب این اپلیکیشن را به صورت دقیق و با جزییات آماده کرده است که به شما کمک می‌کند تا وضعیت امنیتی و شبکه‌ی مورد استفاده خود را در ایران تنظیم کنید.

مزایا و ویژگی‌ها

«تور» شما را گمنام نگه داشته و اطمینان حاصل می‌کند که داده‌های شما از چشم سازمان‌های خصوصی و دولتی که بخواهند بر آن‌ها نظارت کنند، مخفی بماند. «تور» یک فناوری است که امتحان خود را پس داده و ثابت کرده که در این زمینه و همینطور در زمینه‌ی دور زدن فیلترها موثر عمل می‌کند.

همچنین استفاده از این اپلیکیشن سبب میشود که سرویس‌دهنده اینترنت شما نتواند داده‌های مربوط به الگوهای فعالیت شما را در اینترنت برای فروش به تبلیغ کنندگان، جمع‌آوری کند.

از نسخه ۱۱.۵ به بعد در این اپلیکیشن تمهیداتی برای دور زدن راحتتر فیلترینگ و سانسور در نظر گرفته شده است. این نسخه به طور خودکار و بر اساس موقعیت محلی شما، مناسبت‌ترین پل‌ها را برای دور زدن فیلترینگ انتخاب می‌کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

ایران تلاش زیادی برای فیلتر کردن «تور» داشته است و باعث شده که وصل شدن به اینترنت از ایران نسبت به کشورهای دیگر با چالش‌های بیشتری روبه‌رو باشد.همچنین باید توجه داشت که در هنگام استفاده از «تور» با پایین آمدن سرعت اینترنت مواجه خواهید شد.هر چند این اپلیکیشن در حفظ امنیت شما بی‌مانند است، اما این موضوع به قیمت پایین آمدن سرعت تمام می‌شود.

محتوای ترافیک شما به وسیله «تور»محافظت می‌شود اما برای ماموران حکومتی کار چندان سختی نیست که متوجه استفاده شما از «تور» بشوند.حواستان باشد که این موضوع می‌تواند فعالیت‌های شما را در معرض سوءظن قرار دهد.

OrBot

Android | iOS | F-Droid

«اوربوت» یک اپلیکیشن پروکسی رایگان است که کمک می‌کند اپلیکیشن‌های دیگر به شکل امن‌تری از اینترنت استفاده کنند. «اوربوت» از «تور» استفاده می‌کند تا ترافیک اینترنتی شما را رمزگذاری کند و سپس آن را به کامپیوترهای متعددی در نقاط مختلف دنیا می‌فرستد و از این طریق داده‌های ترافیک شما را مخفی نگه می‌دارد.

سهولت استفاده

می‌توانید نسخه‌ی اندروید این اپلیکیشن را از لینک‌های بالا دانلود کنید. برای بعضی مدل تلفن‌های گلکسی سامسونگ، چند مرحله‌ی اضافی وجود دارد تا این اپلیکیشن فعال شود. این مراحل در این ویدیو توضیح داده شده است.

مزایا و ویژگی‌ها

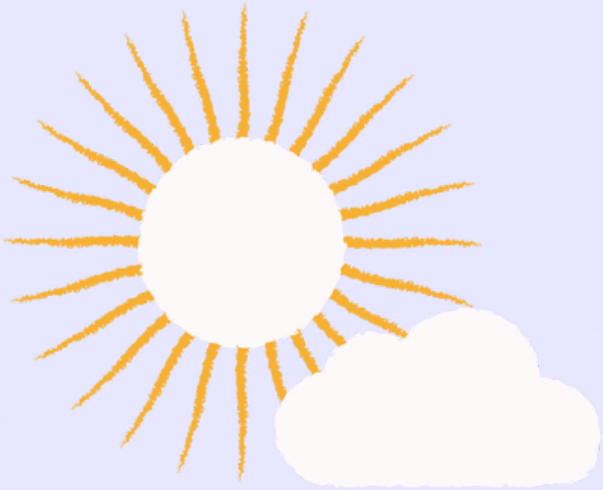
استفاده از «تور» می‌تواند شما را در برابر نظارت و شنود روزمره محافظت کند. زمانی که از «اوربوت» استفاده می‌کنید، ترافیک شما در حین گذشتن از شبکه‌ی «تور»، سه نوبت رله و رمزگذاری می‌شود، و به این وسیله یکی از قوی‌ترین روش‌های ممکن حفاظتی و گمنام ماندن در فضای آنلاین فراهم می‌گردد.

ویژگی دیگر این است که در داخل این اپلیکیشن، شما می‌توانید اپلیکیشن‌های دیگری را که می‌خواهید به دست «تور» محافظت شوند انتخاب کنید. این کار به این معنا است که سرعت اپلیکیشن‌ها و فعالیت‌های غیرحساس، بی‌دلیل پایین نخواهد آمد، مسئله‌ای که در مورد کار با «تور» از عوارض جانبی آن محسوب می‌شود.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

همانطور که در بالا اشاره شد، در برخی مدل‌های تلفن همراه لازم است که از چند مانع فنی اضافی برای فعال کردن این اپلیکیشن گذر کرد. همانند دیگر ابزارهایی که از طریق «تور» حفاظت می‌شوند، این اپلیکیشن نیز سرعت اتصال شما را پایین می‌آورد.

محتوای ترافیک شما به وسیله «تور» محافظت می‌شود اما برای ماموران حکومتی کار چندان سختی نیست که متوجه استفاده شما از «تور» بشوند. حواستان باشد که این موضوع می‌تواند فعالیت‌های شما را در معرض سوءظن قرار دهد.



جعبه‌ابزار اختلال در اینترنت

هیچ‌وقت شده احساس کنید به زمانی برگشته‌اید که با مودم‌های ۵۶کا به اینترنت وصل می‌شدید؟ آیا از دیدن پیام «در حال بارگذاری» خسته شده‌اید؟ آیا جان به‌لب می‌شوید تا پیام‌هایتان ارسال شوند؟
کاملا می‌فهمیم چه حسی دارد.
پایین آمدن سرعت اینترنت مسئله‌ای غیرعادی نیست. گاهی به دلیل زیرساخت شبکه‌ای ضعیف، گاهی به دلیل تعمیرات و به‌روزرسانی، و گاهی به این دلیل که مسئولان به صورت عمدی پهنای باند را مسدود می‌کنند تا دسترسی مردم به اطلاعات را قطع کنند.
وقوع این اختلالات رو به افزایش است. به تازگی در نقاط مختلف ایران، سرعت اینترنت به دفعات برای چندین روز به صورت چشمگیری پایین آمده یا حتی برای چندین ساعت متوالی کاملا قطع شده است.
کار چندانی برای جلوگیری از این اتفاقات نمی‌توان انجام داد، اما می‌توانید ابزارهایی در چنته داشته باشید تا در صورتی که سرعت اینترنت (و یا شبکه ملی اطلاعات) پایین آمد، بتوانید برای برقراری ارتباط با خانواده، دوستان و کانتکت‌های مهم خود از این ابزار استفاده کنید و یا به اطلاعات ضروری دسترسی پیدا کنید.
جعبه‌ابزار اختلال ما شامل راهنمایی‌هایی درباره برخی از این ابزارها است که می‌توانند در زمان اختلال‌های متناوب در اتصال به اینترنت، به شما کمک کنند. این ابزارها به شما اجازه می‌دهند تا اطلاعات را بدون دسترسی به اینترنت مناسب به اشتراک بگذارید، و یا روی شبکه‌های محلی به صورت رمزگذاری شده، ارتباط برقرار کنید و فایل به اشتراک بگذارید.

اپلیکیشن‌های پیام‌رسان – سرعت فرستادن این پیغام برای شما تا چه حد ضروری است؟

حتی اگر سرعت اینترنت شما بسیار پایین باشد، اپلیکیشن‌های پیام‌رسان رمزگذاری شده همچنان عمل خواهند کرد، البته ممکن است در فرستادن و دریافت پیام‌ها با تاخیر بسیار طولانی مواجه شوید.
انتخاب اپلیکیشن مناسب در این موقعیت به این سوال بستگی دارد که چقدر سریع باید این پیغام را بفرستید. آیا تاخیر در فرستادن پیام یا فایل برایتان مسئله خاصی نیست، یا اینکه فایل شما باید فوراً بدون هیچ تاخیری ارسال شود؟
ضروری نیست، می‌توان صبر کرد.
اپلیکیشن «سیگنال» همچنان ساده‌ترین گزینه برای استفاده در زمان وقوع اختلال در اینترنت است. این اپلیکیشن مطمئن و امن است، و هر چند که احتمالا با تاخیر مواجه خواهید بود، اما برقراری ارتباط را ممکن می‌سازد.

Signal

Android | iOS | Windows | Linux

«سیگنال» اپلیکیشن پیام‌رسانی با قابلیت رمزگذاری سرتاسری E۲EE است که از سیستم‌عامل‌های iOS، اندروید، ویندوز و لینوکس پشتیبانی می‌کند. این اپلیکیشن رایگان بوده و به عنوان یکی از ایمن‌ترین اپلیکیشن‌های پیام‌رسان موجود از سوی موسساتی چون Electronic Frontier Foundation و Access Now توصیه می‌شود.

این اپلیکیشن به کاربران خود اجازه می‌دهد تا پیام‌های ویدیویی، صوتی، نوشتاری و عکس را به صورت گروهی و رمزگذاری شده ارسال کنند. همچنین امکان تماس‌های تلفنی با قابلیت رمزگذاری سرتاسری برای کاربران «سیگنال» وجود دارد.

سهولت استفاده

شما می‌توانید «سیگنال» را برای سیستم‌های اندروید و iOS با استفاده از لینک‌های بالا بلافاصله دانلود کنید. کار با این اپلیکیشن بسیار ساده است. وقتی اپلیکیشن را باز می‌کنید، از شما خواسته می‌شود تا شماره تلفن خود را از طریق یک کد شش رقمی تایید کنید، که این کد با اس‌ام‌اس برای شما ارسال می‌شود.

وقتی این کار را انجام دادید، بلافاصله می‌توانید مکاتبات خود را با هر کدام از کانتکت‌های خود - به شرط آن‌ها هم اپلیکیشن سیگنال را دانلود کرده باشند- شروع کنید.

از اردیبهشت ۱۴۰۱ قابلیت جدیدی به سیگنال اضافه شده است که در صورت تغییر سیم کارت نیازی به اجرای دوباره برنامه نیست و اپلیکیشن شمابا همان اطلاعات قبلی و تنها با شماره جدید قابل استفاده است.

مزایا و ویژگی‌ها

سیستم رمزگذاری «سیگنال» بسیار مطمئن است، این اپلیکیشن، منتخب ادوارد اسنودن است.

سیگنال فقط پیام‌های شما را رمزگذاری نمی‌کند، بلکه فراداده‌ها را نیز پنهان می‌کند تا اطمینان حاصل شود که هیچ‌کس، نه حتی خود سیگنال یا هرکس که سعی کند تا جلوی پیام‌های شما را بگیرد، نتواند فرستنده و گیرنده پیام‌ها را شناسایی کند.

همچنین سیگنال یک اپلیکیشن متن‌باز است، این بدین معنی است که کد آن برای مشاهده همگان و کسانی که تلاش کنند آن را بشکنند، در دسترس است. تا به امروز پروتکل رمزگذاری سیگنال هرگز شکسته نشده است.

سیگنال داده‌های شما یا هیچ‌کس دیگری را جمع‌آوری نمی‌کند و به اشتراک نمی‌گذارد.

همچنین این اپلیکیشن از تیر ماه ۱۴۰۰ به بعد، از پروکسی‌های مخصوص به خود پشتیبانی می‌کند. برای دستیابی به این پروکسی‌ها می‌توانید هشتگ #IRanASignalProxy را در توئیتر دنبال کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

«سیگنال» از شماره تلفن شما برای ثبت‌نام و همینطور به عنوان شناسه‌ی شما استفاده می‌کند. به همین دلیل باید مواظب باشید که از این اپلیکیشن تنها برای برقراری ارتباط با کانتکت‌های قابل اعتماد خود استفاده کنید.

اگر تصمیم می‌گیرید که از «سیگنال» به عنوان اپلیکیشن پیش‌فرض برای فرستادن پیامک استفاده کنید، یادتان باشد که پیام‌های شما تنها در صورتی رمزگذاری می‌شوند که گیرنده نیز اپلیکیشن سیگنال را روی تلفن همراه خود نصب کرده باشد.

مورد دیگر اینکه، «سیگنال» تنها در صورت دسترسی به اینترنت به کار می‌آید. هر چند که ابزاری عالی برای استفاده روزمره است، در صورت قطع شدن اینترنت خیلی کارایی نخواهد داشت.

Session

Android | iOS | Windows | Linux

سِشِن (Session) یک پیام رسان امن با قابلیت رمزگذاری سرتاسری است که به کاربران خود اجازه می‌دهد پیام‌های ویدیویی، صوتی، نوشتاری و عکس را به صورت گروهی و رمزگذاری شده ارسال کنند. حفظ حریم خصوصی کاربر در طراحی این اپلیکیشن جایگاه ویژه‌ای داسته است؛ این برنامه برای ثبت نام نیازی به شماره تلفن ندارد و هیچ داده و یا فراداده‌ای را در خود نگه نمی‌دارد. اپلیکیش سشن که از جدیدتری پیام‌رسان‌های موجود است، کاملا رایگان و متن باز است که این باعث بررسی عمومی و رفع نقص مداوم در آن می‌شود. این برنامه مبتنی بر کلید عمومی است و از سرورهای غیر متمرکز استفاده می‌کند.

سهولت استفاده

همانطور که گفته شد این اپلیکیش برای ایجاد حساب کاربری نیازی به شماره تلفن همراه ندارد. همچنین احراز هویت و شناسایی فرد صاحب حساب در این اپلیکیشن ضروری نیست و نام کاربری شما می‌تواند هر نامی اعم از واقعی یا مستعار باشد. پس از نصب، این برنامه یک کد دراختیار شما خواهد گذاشت. برای اضافه کردن دیگران به لیست مخاطبان خود کافی است این کد را در اختیار آن‌ها قرار دهید.

مزایا و ویژگی‌ها

در این پیام‌رسان شما می‌توانید یک حساب کاربری را در چند دستگاه مختلف همگام‌سازی کنید. همچنین این امکان وجود دارد که با رمز اولیه که برنامه در هنگام نصب در اختیار شما میگذارد پس از پاک شدن احتمالی، حساب خود را بازیابی کنید. هیچ ابرداده‌ای از جمله نوع دستگاه و یا IP شما در این برنامه جمع‌آوری نمی‌شود بنابراین و اساسا داده‌هایی از این دست برای رصد کردن احتمالی وجود ندارد. از طرفی با رعایت پروتکل رمزگذاری سرتاسری، ناشناس ماندن فرستنده و گیرنده در در این برنامه لحاظ شده است. سشن از شفافیت کافی برخوردار است و سیستم کد گذاری آن برای حساب‌رسی در اختیار عموم قرار گرفته است. سشن به شما امکان داشتن گروه‌های عمومی تا حداکثر بیست نفر را می‌دهد و همزمان می‌توانید گروه‌های خصوصی‌تری از دوستان نزدیک را هم در این برنامه ساماندهی کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

با اینکه سشن یک ابزار امن و قدرتمند برای برقراری ارتباط است، اما به نظر نمی‌رسد که در حال حاضر برای مصرف کننده‌های عمومی مناسب باشد و بیشتر قابل استفاده برای افرادی است که بتوانند برخی پیچیدگی‌های کار با آن را مدیریت کنند.

امکان برقراری تماس صوتی و ویدیویی در این برنامه وجود ندارد و حداکثر حجم تبادل فایل در آن ۱۰ مگابایت است.

از معایب این برنامه می‌توان نداشتن گزینه‌ی تائید دو مرحله‌ای است را بر شمرد. همچنین و به نسبت اپلیکیشن‌هایی از این دست امکان شخصی سازی محیط در آن بسیار محدود است.

Jami

Android | iOS | Windows | Linux

«جمی» پلتفرم رایگان برای ارتباط و مکاتبه است که ادعا می‌کند هویت و حریم خصوصی کاربران خود را حفاظت می‌کند. «جمی» دارای رمزگذاری سرتاسری است و به شکل همتا به همتا عمل می‌کند، بنابراین نیازی به یک سرور مرکزی برای انتقال داده بین کاربران ندارد.
به همین سبب، کاربرانی که روی یک شبکه‌ی محلی مشترک هستند (برای مثال، یک شبکه وای‌فای عمومی بدون دسترسی به اینترنت) باید بتوانند از طریق «جمی» به هم متصل شوند، حتی اگر به اینترنت وصل نباشند.

سهولت استفاده

دانلود این اپلیکیشن برای اندروید از گوگل‌پلی، و برای iOS از اپل استور امکانپذیر است. نسخه‌های مخصوص دسکتاپ (مک، ویندوز و لینوکس) را هم می‌توان از خود وبسایت «جمی» دانلود کرد.
برای ایجاد حساب جمی نیازی به ارائه هیچ مشخصات فردی و یا حتی شماره تلفن نیست.

مزایا و ویژگی‌ها

علاوه بر برقراری ارتباط امن، «جمی» تماس‌های ویدویی و کنفرانسی با کیفیت اچ‌دی را نیز ارائه می‌کند، اما کیفیت این تماس‌ها بسیار بستگی به کیفیت اینترنت مورد استفاده دارد.
داشتن قابلیت ارسال پیام از طریق شبکه‌های وای‌فای می‌تواند در زمان‌های قطع موقت اینترنت (و حتی قطع کامل اینترنت) به منظور برقراری ارتباط با کانتکت‌هایی که در نزدیکی شما هستند، موثر عمل کند. «جمی» همچنین ممکن است بتواند در صورت محدود شدن دسترسی به اینترنت جهانی به شکلی مطمئن عمل کند، اما تنها در صورتی که اینترنت ملی در دسترس باقی بماند.
به این موضوع توجه داشته باشید که محققان ما به صورت مستقل قادر به تایید این گزارش‌ها نبوده‌اند، بنابراین نمی‌توانند درباره کارکرد این اپلیکیشن در چنین شرایطی با قطعیت نظر بدهند. آزمایش‌ها و شواهد بیشتری برای این کار نیاز است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

بر خلاف برخی از اپلیکیشن‌هایی که بر پایه‌ی شبکه توری meshnet-based طراحی می‌شوند، «جمی» قادر به استفاده از بلوتوث برای برقراری ارتباط با دستگاه‌های دیگر نیست. برقراری ارتباط آفلاین با کانتکت‌ها، نیازمند اتصال هر دو طرف به یک شبکه‌ی اینترنت مشترک محلی است.
همچنین سازندگان راهی برای درخواست از بین بردن کامل اطلاعات در این اپلیکیشن در نظر نگرفته‌اند.

Briar

Android | F-Droid app

«برایر» یک اپلیکیشن پیام‌رسان است که برای استفاده کنشگران، روزنامه‌نگاران و هر کس دیگری که احتیاج به برقراری ارتباط در زمان قطع اینترنت داشته باشد، طراحی شده است. برخلاف اپلیکیشن‌های پیام‌رسان سنتی، «برایر» متکی بر یک سرور مرکزی نیست، پیام‌ها با استفاده از یک شبکه توری به صورت مستقیم بین دستگاه‌های کاربران همزمان‌سازی یا همان synchronized می‌شوند.

سهولت استفاده

کاربران می‌توانند «برایر» را برای اندروید از پلی استور گوگل، F-Droid یا وب سایت برایر دانلود نمایند..

مزایا و ویژگی‌ها

«برایر» می‌تواند برای به اشتراک گذاشتن پیام‌های مهم با افرادی که به آن‌ها اعتماد دارید، به شکلی مطمئن عمل کند. در هنگام قطع شدن اینترنت، این اپلیکیشن اجازه می‌دهد تا داده‌ها و اطلاعات را با لیست مخاطبان(کانتکت‌ها) خود به شکلی امن به اشتراک بگذارید، البته لازم خواهید داشت تا با فرد گیرنده در محدوده‌ی بلوتوث یا روی یک شبکه وای‌فای مشترک قرار داشته باشید.

علاوه بر قابلیت گپ زدن سرتاسری خصوصی و گروهی، «برایر» به شما این امکان را می‌دهد تا تالارهای گفتگوی عمومی و بلاگ‌هایی تشکیل دهید که برقراری ارتباط را با گروه‌های معتمد میسر می‌سازد، و حتی در زمان‌های قطع اینترنت هم قابل اشتراک‌گذاری و به‌روزرسانی هستند.

تالارهای گفتگو، مکالمات غیر خصوصی هستند. بر خلاف گروه‌های خصوصی، هر کسی که به آن بپیوندد می‌تواند کانتکت‌های دیگر خود را به تالار دعوت کند. در ضمن بلاگ‌ها امکان پست و به اشتراک گذاشتن اخبار و بروزرسانی‌ها را با تمام کانتکت‌هایتان امکان پذیر می‌سازند.

«برایر» همچنین با اپلیکیشن "دکمه هشدار" Ripple مجهز شده است که می‌تواند برایر را مخفی کند یا در حالتی که نگران هستید حساب کاربری شما تحت نظارت قرار گرفته یا مصادره شده، می‌تواند طوری پیکربندی شود که حساب کاربری و تاریخچه پیغام‌های شما را پاک کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

این اپلیکیشن البته اشکالاتی نیز دارد. گزارش‌هایی از مشکلات برقراری ارتباط از طریق بلوتوث در زمانی که اینترنت قطع شده است دریافت شده، اما گروه «برایر» مشغول رفع این اشکالات هستند.

در زمان قطع اینترنت، این اپلیکیشن تنها در صورتی که کاربران در محدوده بلوتوث و وای‌فای یکدیگر قرار داشته باشند، می‌تواند کارایی داشته باشد.

مشکل دیگر این اپلیکیشن این است که تا زمانی که تعداد زیادی از افراد شروع به استفاده از «برایر» نکنند، نمی‌تواند در زمان‌های قطع دسترسی به اینترنت از تمام امکانات بالقوه خود استفاده کند و موثر واقع شود. برای اینکه «برایر» بتواند به یک اپلیکیشن پیام‌رسان قدرتمند تبدیل شود و جایگزین پیام‌رسان‌های معمول بشود، می‌بایست تعداد کاربران گسترده‌ای را جذب کند.

Nahoft

Android

«نهفت» که در فارسی به معنی پنهان است، یک نرم‌افزار آفلاین رمزنگاری پیام و حفظ حریم‌خصوصی برای استفاده در شبکه‌های ناامن است. در واقع «نهفت» یک پیام‌رسان نیست اما با رمزنگاری پیام‌ها، دسترسی دیگران به محتوای رد و بدل شده توسط شما و دوستان‌تان در دیگر پیام‌رسان‌ها را غیر ممکن می‌کند.
این برنامه توسط گروه حقوق بشری اتحاد برای ایران و در قالب پروژه‌ی ایران کوباتور ۲ توسعه داده شده است. سازمان اتحاد برای ایران یک نهاد حقوق بشری است که مرکز آن در شهر برکلی، ایالت کالیفرنیا قرار دارد. هدف این نهاد گسترش آزادی‌های مدنی در ایران، دفاع از حقوق بشر، حمایت از جامعه مدنی و ترغیب به مشارکت از طریق فناوری است.

سهولت استفاده

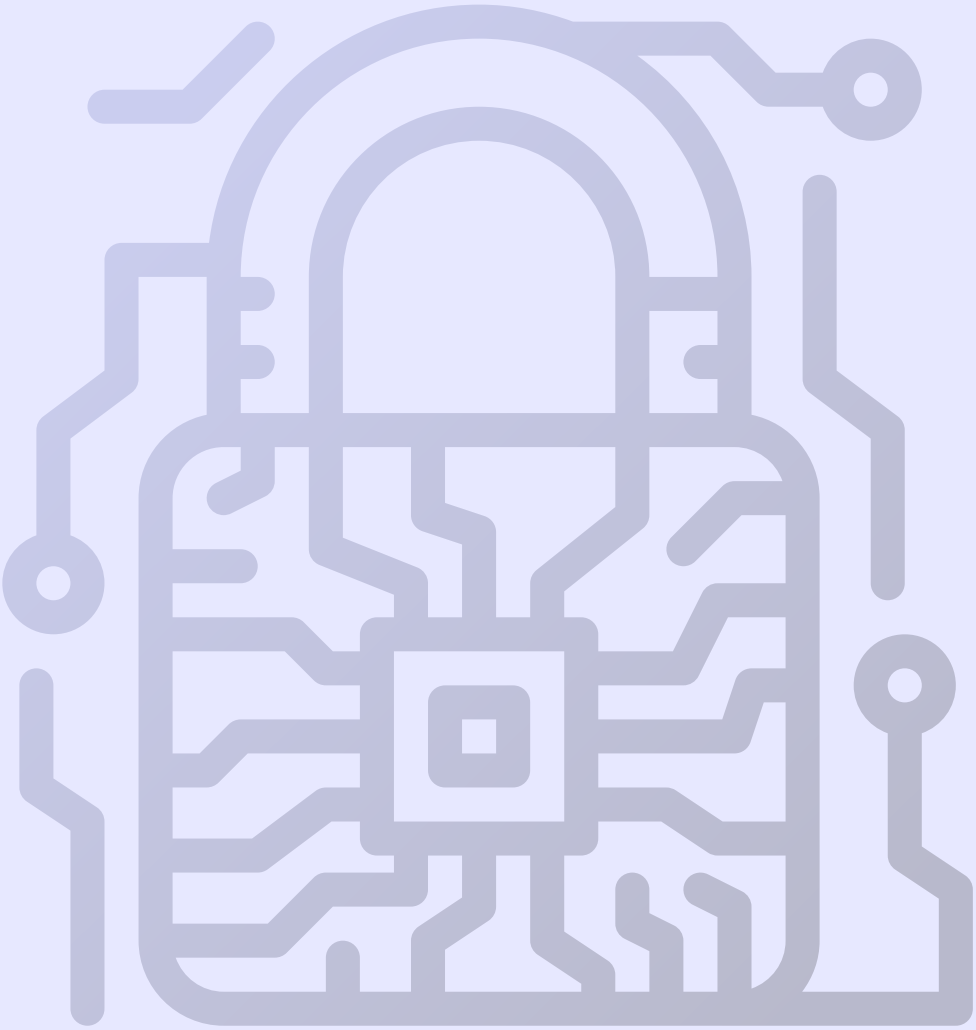
این نرم افزار متن باز که با تکنیک پنهان‌نگاری (Steganography) طراحی شده، کاملا آفلاین است و از هیچ سروری جهت ارسال یا دریافت یا رمزگذاری پیام‌های شما استفاده نمی‌کند.
شما می‌توانید متن خود را رمزگذاری کنید و آن را از طریق متن، کلمات شانسی یا انتخاب یک تصویر از گالری دستگاه خودتان ارسال کنید.
شما همچنین می‌توانید یک پیام را رمزگذاری کنید، آنرا در یک تصویر بگنجانید و در حافظه دستگاه خود نگهداری کنید.
در عین حال این امکان وجود دارد که پس از رمزگشایی و خواندن پیام دریافتی آن را در نهفت ذخیره کنید و یا در همان لحظه آن را پاک کنید.
همچنین این برنامه دارای قابلیت تعریف یک کد ورود تخریبی است. ایجاد این کد به شما کمک میکند که در زمان اضطرار و هنگامی که احتمال دسترسی دیگران به گوشی تلفن همراه شما ممکن است از آن استفاده کرده و تمام اطلاعات ذخیره شده در این نرم افزار را در یک لحظه پاک کنید.
نهفت در دو مرحله توسط پژوهشگران و متخصصان Cure۵۳ ارزیابی امنیتی شده و پیش از انتشار آخرین نسخه، پیشنهادات آنان برای بهبود امنیت اپ به کار گرفته شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از آنجایی که اصولا فرآیند رمزنگاری فرآیند پیچیده‌ای است ممکن است استفاده از این برنامه برای تمام کاربران ساده نباشد. همچنین برخی کاربران از پیچیده بودن رابط کاربری این برنامه گلایه کرده‌اند.
این برنامه تا کنون تنها برای سیستم عامل اندروید طراحی شده و نسخه‌ای برای اپل، ویندوز و لینوکس ارائه نکرده است.

ابزارهای دور زدن – انتظار پایین آمدن سرعت را داشته باشید

در صورت کند شدن سرعت اینترنت، باید انتظار این را داشته باشید که ابزارهای دورزدن و وی‌پی‌ان‌های شما از حالت عادی هم کندتر شوند. اگر می‌خواهید به محتوای فیلترشده دسترسی داشته باشید، همچنان باید از یک وی‌پی‌ان استفاده کنید، فقط انتظار معطلی بیشتر را داشته باشید.
حتی اگر وی‌پی‌ان‌های معتمدی که ما در اینجا معرفی می‌کنیم در این شرایط کند شدند، وسوسه نشوید که وی‌پی‌ان‌های رایگان ناشناخته را امتحان کنید. همه‌ی وی‌پی‌ان‌ها امن نیستند و اگر احتیاط نکنید ممکن است گرفتار بدافزارها یا نظارت و شنود ارگان‌ها و شرکت‌ها گرفتار شوید.
اگر هیچ‌کدام از ابزارهای زیر به درستی عمل نکردند و خواستید وی‌پی‌ان دیگری را امتحان کنید، لطفاً از سایت پس‌کوچه دیدن کنید تا لیست کاملی از وی‌پی‌ان‌ها و ابزارهای دور زدن قابل اعتماد را آنجا پیدا کنید.



Psiphon

Android | iOS | Windows | Android direct source

««سایفون» ابزاری برای دور زدن فیلترینگ است که از فناوری‌های وی‌پی‌ان، اس‌اس‌اچ و اچ‌تی‌تی‌پی استفاده می‌کند تا دسترسی بدون سانسور به محتوای اینترنت را برای شما فراهم کند. این اپلیکیشن به صورت خودکار به نقاط دسترسی جدید پی می‌برد تا احتمال دور زدن فیلترها را برای شما بالا ببرد.

سهولت استفاده

کار کردن با «سایفون» خیلی راحت است. فقط لازم است آن را از طریق یکی از لینک‌های بالا روی دستگاه خود دانلود و نصب کنید. بعد از اینکه نصب شد، اپلیکیشن را باز کنید و روی 'connect' بزنید تا «سایفون» روی دستگاه فعال شود..

مزایا و ویژگی‌ها

«سایفون» سابقه‌ی طولانی در دور زدن سانسور اینترنتی در ایران دارد و همچنان برای این منظور کارایی خود را حفظ کرده است.

هر چند در زمان‌های وقوع اختلال در اینترنت و یا قطع کامل از کارایی آن کم می‌شود، بخش کوچکی از کاربران «سایفون» گزارش داده‌اند که طی قطع شدن اینترنت در آبان ۱۳۹۸ به محتوای اینترنت جهانی دسترسی داشته‌اند. تحقیقات مکملی که از سوی«سایفون» صورت گرفت نیز صحت این موضوع را تایید کرد.

در نسخه‌ی ۵.۰ و بالاتر اندروید فیلترشکن سایفون، امکان غیر فعال کردن برنامه‌هایی که نمی‌خواهید از تونل سایفون رد شوند را دارید.

بدین ترتیب می‌توانید از این فیلتر شکن هدفمندتر استفاده کرده و در مصرف حجم اینترنت نیز صرفه جویی کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

باگر دنبال دست یافتن به اطلاعات حساس یا به اشتراک گذاشتن آن هستید، نباید فقط به این اپلیکیشن متکی باشید.

هرچند که با استفاده از «سایفون»، ISP شما قادر به دیدن محتوای در حال داد و ستد شما نخواهد بود، اما این اپلیکیشن مانع این نمی‌شود که تاریخچه مرورگر و کوکی‌ها بر روی دستگاه شما ذخیره نشوند.

توجه داشته باشید که «سایفون» برخی اطلاعات در رابطه با ناحیه، کشور و فعالیت‌های انجام شده روی مرورگر شما و زمان و تاریخ آن ها را ثبت می‌کند. برنامه‌نویسان «سایفون» این داده‌ها را جمع‌آوری و تحلیل کرده و سپس آن‌ها را حذف می‌کنند. خط مشی «سایفون» در رابطه با حفظ حریم خصوصی به زبان فارسی در اینجا موجود است، که در مورد جمع‌آوری داده‌ها و نحوه‌ی به اشتراک گذاشتن آن‌ها با طرف ثالث در آن توضیح داده شده است.

Lantern 

Android| iOS | Windows | GitHub

«لنترن» یک نوع اپلیکیشن دور زدن فیلترینگ است که چندین روش مختلف را برای گذر از فیلتر و سانسور بکار می‌گیرد و بسته به تغییراتی که سانسورچی ایجاد می‌کند، از روشی به روش دیگر می‌رود. این ابزار، فیلتر بودن یا نبودن یک وب‌سایت را تشخیص می‌دهد و تنها در این صورت که وبسایت خارج از دسترس باشد، شروع به استفاده از شیوه‌های دور زدن می‌کند. این امر به این معناست که می‌تواند به وب‌سایت‌های فیلتر نشده سریع‌تر متصل شود.
هر چند اکثر مواقع سرعت بالایی ارائه می‌دهد و داد و ستد داده‌های شما را در وب‌سایت‌های فیلتر شده رمزگذاری می‌کند، اما ادعا نمی‌کند که از هویت کاربران خود حفاظت می‌کند و امکان این را ندارد که کاربران را در برابر نظارت و شنود، مانند اپلیکیشن‌های دیگری مثلاً «تور» Tor، محافظت کند.

سهولت استفاده

کار با «لنترن» نسبتاً سرراست است. فقط لازم است که با استفاده از یکی از لینک‌های بالا روی دستگاه خود دانلود و نصبش کنید. بعد از اینکه نصب شد، اپلیکیشن را باز کنید و connect را بزنید تا فعال شود.

مزایا و ویژگی‌ها

ویژگی اصلی «لنترن» این است که دسترسی به وب‌سایت‌های فیلتر شده را با سرعت بالایی ارائه می‌دهد. در شرایط معمول ایران، این اپلیکیشن معمولاً ثابت کرده که در شکستن فیلترهای حکومتی موثر عمل می‌کند.
به همین دلیل برای استفاده روزمره کاربران معمولی و گذر از فیلترینگ دولتی ایران، مناسب‌ترین ابزار است، اما برای استفاده روزنامه‌نگاران و کنش‌گرانی که فاش نشدن هویت خودشان را باید در اولویت قرار دهند، ابزار مناسبی نیست. اگر حفظ کامل حریم خصوصی و هویت، برای شما موضوع مهمی است، باید به دنبال وی‌پی‌انی باشید که مخصوصاً برای این منظور طراحی شده باشد.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

در آبان ۱۳۹۸ که اینترنت ایران قطع شده بود، «لنترن» آنچنان که باید موثر عمل نکرد و هیچ گزارش موثقی مبنی براینکه کاربران «لنترن» بعد از قطع شدن اینترنت توانسته باشند به اینترنت جهانی وصل شوند، دریافت نشده است. به همین دلیل ما کار با این اپلیکیشن را فقط در وضعیت«عادی» توصیه می‌کنیم.
همانطور که گفته شد، «لنترن» هیچ ادعایی مبنی بر اینکه هویت شما را محفوظ نگه می‌دارد، نداشته است. هر نوع ارتباطی که از طریق «لنترن» ایجاد شده باشد، رمزگذاری می‌شود اما این نرم‌افزار نمی‌تواند هیچ اقدامی در جهت محافظت کاربران در برابر وبسایت‌هایی که کاربران خود را رصد می‌کنند یا در برابر نظارت و شنود حکومتی، انجام دهد.
«لنترن» اطلاعات شخصی مربوط به ناحیه، کشور و فعالیت‌های انجام شده روی مرورگر شما و زمان و تاریخ آن ها را ثبت می‌کند. این داده‌ها پیش از آن که از طرف برنامه‌نویسان این نرم‌افزار تحلیل شوند، جمع‌آوری aggregate می‌شوند و تنها در حالتی با طرف ثالث به اشتراک گذاشته می‌شوند که کاملا aggregate و گمنام‌سازی شده باشند.
اطلاعات بیشتر در بخش «خط مشی در زمینه حریم خصوصی» لنترن در اینجا به زبان انگلیسی موجود است.

Proton VPN

Android | iOS | Windows | Linux

«پروتون وی‌پی‌ان» یک رساننده خدمات شبکه مجازی خصوصی است که با پشتوانه مالی جمعی حمایت می‌شود و از سوی بنیانگذاران خدمات امنیت ایمیل «پروتون میل» عرضه شده است. این اپلیکیشن محافظت از امنیت و حریم خصوصی کاربران را در سطح بسیار بالایی تامین می‌کند.
نکته‌ی بسیار مهم این است که «پروتون وی‌پی‌ان» نسخه‌ی رایگانی از خدمات خود را بدون هیچ محدودیت در ترافیک داده، به کاربران این رده ارایه می‌دهد.
این وی‌پی‌ان که ۱۷۰۰ سرور در ۶۰ کشور جهان دارد با نرخ انتقال داده‌ی ۶۰ مگابایت بر ثانیه از سرعت قابل قبولی نیز برخوردار است هر چند نمیتوان مطمئن بود که شما در نسخه رایگان نیز از همین سرعت برخوردار باشید.

سهولت استفاده

روند ثبت‌نام بسیار سرراست است. اگر از وی‌پی‌ان دیگری دارید استفاده می‌کنید، به وبسایت «پروتون وی‌پی‌ان» بروید و با ایمیل خود یک حساب کاربری باز کنید، سپس نام کاربری و کلمه‌ی عبور خود را انتخاب کنید. بعد از آن دیگر می‌توانید نسخه‌ی مناسب دستگاه خود را دانلود کنید.

مزایا و ویژگی‌ها

روش کار «پروتون وی‌پی‌ان» بر این اساس است که هیچ داده‌ای را ثبت نکند، و خط مشی مکتوب بسیار دقیق و واضحی دارد که می‌توانید آن را به زبان انگلیسی در اینجا بخوانید. این اپلیکیشن طوری طراحی شده که یک تونل رمزگذاری شده بین شما و سرورهای خود ایجاد می‌کند، و با این کار از شما در برابر نظارت و شنود دشمنان محافظت کرده و تاریخچه فعالیت‌های شما را از آی‌اس‌پی مخفی نگه می‌دارد.
اپلیکیشن‌های «پروتون وی‌پی‌ان» روی همه‌ی پلتفرم‌ها کاملاً متن‌باز هستند و امنیت آن‌ها به صورت مستقل بررسی دقیق شده است. این وی‌پی‌ان همچنین دارای قابلیت قطع اضطراری (kill switch) است که در صورت قطع شدن وی‌پی‌ان، جلوی ترافیک اینترنت را بر روی دستگاه شما می‌گیرد. این موضوع باعث می‌شود که تصادفا بدون محافظت نمانید.
سرورهای «پروتون وی‌پی‌ان» در سوئیس مستقر هستند، کشوری که قوانین سفت و سختی در زمینه‌ی حفاظت از حریم خصوصی دارد و سابقه نشان داده که در برنامه‌های اشتراک‌گذاری اطلاعات و جاسوسی بین‌المللی وارد نمی‌شود.
بر اساس این قوانین و ویژگی‌ها، می‌توان گفت که «پروتون وی‌پی‌ان» دارای کارنامه‌ای قوی در زمینه‌ی حریم خصوصی، امنیت و رمزگذاری است و اگر به دنبال وی‌پی‌ان رایگان هستید می‌تواند انتخاب خوبی باشد..

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

برای استفاده از «پروتون وی‌پی‌ان» لازم است که حتما در آن ثبت‌نام کنید که این موضوع ممکن است چالش‌هایی را در مواقع اختلال اینترنت یا وقتی که وب‌سایت اپلیکیشن فیلتر شده باشد، به وجود آورد. توصیه می‌شود که برای ثبت‌نام از آدرس ایمیلی غیر از آدرس همیشگی خود استفاده کنید.
همانند دیگر وی‌پی‌ان‌های تجاری، بسته‌ی رایگان «پروتون وی‌پی‌ان» به احتمال زیاد نسبت به نسخه‌های پولی آن، تأثیرات منفی زیادی روی سرعت اینترنت شما خواهد داشت. هر چند این اپلیکیشن ابزاری مهم و کارآمد برای حفاظت از هویت شما و گذر از فیلترها است، این موضوع می‌تواند به قیمت پایین آمدن سرعت اینترنت تمام می‌شود.

TunnelBear

Android| iOS| Windows

«تونل بر» سرویس وی‌پی‌انی است که می‌توانید برای گشت و گذار در اینترنت به شکل محرمانه و امن استفاده کنید. وی‌پی‌ان مطمئن«تونل بر»حریم خصوصی آنلاین شما را حفظ کرده و از طریق استفاده از یک شبکه‌ی خصوصی مجازی(Virtual Private Network – VPN) موقعیت مکانی شما را از دسترس خارج می‌کند. در این روش، اطلاعات به صورت رمزگذاری‌شده به سرور وی‌پی‌ان منتقل می‌شوند و از آن جا به سایت مقصد می‌رسد.نکته‌ی مهم این است که «تونل بر» دارای بسته‌ی رایگانی برای کاربران ایرانی است. این بسته شامل ۱۰ گیگابایت سرویس رایگان در ماه برای کاربران درون ایران است. این اپلیکیشن از چند حسابرسی امنیتی مستقل سربلند بیرون آمده و بنابراین باید بتواند در حفظ امنیت و حریم خصوصی شما در فضای آنلاین موثر واقع شود.

سهولت استفاده

اپلیکیشن «تونل بر» را می‌توانید با استفاده از یکی لینک‌های بالا، مناسب با نوع سیستم‌عامل خود دانلود کنید.
پس از اینکه اپلیکیشن را باز کردید، لازم است که با ایمیل خود یک حساب کاربری بسازید (ما توصیه می‌کنیم از آدرس ایمیل همیشگی خود استفاده نکنید). پس از آن می‌توانید به وی‌پی‌ان متصل شوید.

مزایا و ویژگی‌ها

«تونل بر» بر اساس این سیاست عمل می‌کند که هیچ داده‌ای ثبت نشود، به این معنی که داده‌های مرتبط با آدرس IP شما و یا وب‌سایت‌هایی را که بازدید می‌کنید، ذخیره نمی‌کند. خط مشی مربوط به حریم خصوصی این اپلیکیشن را می‌توانید به زبان انگلیسی دراینجا خوانید که جزییات جامعی درباره‌ی شیوه‌های جمع‌آوری داده به شکل محدود و بدون افشای هویت در آن ارائه شده است.
همانطور که اشاره شد، این اپلیکیشن از چندین حسابرسی امنیتی مستقل سربلند بیرون آمده و بر همین اساس می‌توانیم بگوییم که ابزاری معتبر است و قابلیت‌های آن در زمینه حفظ هویت و حریم خصوصی و همینطور دور زدن فیلترینگ ثابت شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

«تونل بر» در حال حاضر در بسته‌ی رایگان خود تا سقف ۵۰۰ مگابایت در ماه محدودیت استفاده دارد. این موضوع به این معنی است که نباید برای دسترسی به محتوای سنگین مثل تعداد زیاد عکس و فیلم، به این اپلیکیشن متکی بود.
همچنین این سرویس از شما می‌خواهد تا با ایمیل خود در آن ثبت‌نام کنید که می‌تواند در زمان اختلال و قطع شدن اینترنت و یا فیلترینگ، مشکل‌زا شود. علاوه بر این، به شما توصیه می‌شود که از آدرس ایمیل همیشگی خود برای ثبت‌نام استفاده نکنید.

Windscribe VPN

Android | iOS | Windows | Linux

«ویندسکرایب» یک سرویس وی‌پی‌ان تجاری است که می‌توانید برای گشت و گذار آزادانه و امن در اینترنت از آن استفاده کنید. از حریم خصوصی شما محافظت می‌کند و به شما کمک می‌کند تا فیلترهای اینترنتی را دور بزنید.
بسته‌ی رایگان «ویندسکرایب» در هر ماه ۱۰ گیگابایت ترافیک داده ارائه می‌دهد که بسیار دست و دلبازانه است.
همچنین فایروال «ویندسکرایب» روی این بسته موجود است که ادعا می‌کند تمام اتصالات را خارج از تونل خودش می‌بندد تا هیچ داده‌ای از ارتباط شما به بیرون درز نکند.

سهولت استفاده

این اپلیکیشن را از یکی از لینک‌های بالا دانلود کنید. وقتی برای اولین بار اپلیکیشن را باز می‌کنید، از شما خواسته می‌شود تا یک حساب کاربری بسازید. یک آدرس ایمیل و کلمه‌ی عبور انتخاب کنید (ترجیحا آدرس اصلی شما نباشد)، حالا این فرصت را دارید تا ۱۰ گیگابایت ترافیک ماهانه رایگان خود را طلب کنید.
بعد از اینکه این کار را انجام دادید، می‌توانید وی‌پی‌ان را روی دستگاه خود فعال کنید.

مزایا و ویژگی‌ها

هر چند که سرعت این اپلیکیشن ممکن است همیشه به خوبی وی‌پی‌ان‌های دیگر نباشد، اما نشان داده که در ایجاد دسترسی کاربران ایرانی به محتوای فیلترشده بسیار موثر عمل می‌کند.
فایروال موجود در این اپلیکیشن نیز یک لایه‌ی محافظت دیگر به حریم خصوصی اضافه می‌کند تا از خطر نشت اطلاعات از تونل وی‌پی‌ان شما جلوگیری کند.
این اپلیکیشن قابلیت تقسیم تونل را دارد که به شما امکان می‌دهد به طور خاص انتخاب کنید کدام برنامه‌ها از وی‌پی‌ان استفاده کنند. این به معنی صرفه‌جویی قابل توجه در مصرف اینترنت شماست.
از مزایای دیگر این وی‌پی‌ان امکان انتخاب میان چهار پروتکل OpenVPN UDP/TCP, IKEv۲, Stealth است که به سرعت و امنیت وبگردی شما کمک میکند

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

همچون دیگر وی‌پی‌ان‌های تجاری، «ویندسکرایب» نیز به احتمال زیاد در صورت قطع شدن مستمر اینترنت، اختلال در آن و یا پایین آمدن سرعت، خیلی خوب کار نخواهد کرد.
هرچند که می‌تواند ابزار بسیار مفیدی برای رد شدن از فیلترها باشد، اما باید توجه داشته باشیم که به اندازه‌ی ابزارهای دور زدن برگرفته از Tor ، در حفظ هویت شما موثر عمل نخواهد کرد.

1.1.1.1 + WARP

Android | iOS | Windows | LINUX

اپلیکیشن ۱.۱.۱.۱ شرکت Cloud-flare یک برطرف‌کننده‌ی دی‌ان‌اس است که تقریباً شبیه وی‌پی‌ان عمل می کند. ترافیک اینترنت شما را از یک تونل مطمئن رد کرده، رمزگذاری کرده و ادعا می‌کند که داده‌های مرورگر شما را به طرف ثالث نشان نمی‌دهد.
هر چند که احتمالا از نظارت ISP شما بر وب‌سایت‌هایی که باز می‌کنید جلوگیری می‌کند، اما باعث نمی‌شود که اتصال شما به وب‌سایت‌ها بدون فاش شدن هویت شما اتفاق بیفتد، و همچنین قادر نیست سانسورها را به خوبی وی‌پی‌ان دور بزند. البته می‌تواند در حد ابتدایی امنیت فضای آنلاین شما را فراهم کند و در عین حال سرعت قابل قبولی داشته باشد، اما این اپلیکیشن به اندازه‌ی وی‌پی‌ان‌هایی که مخصوص امنیت حریم خصوصی ساخته شده‌اند، موثر نخواهد بود.

سهولت استفاده

شما می‌توانید ۱.۱.۱.۱ + WARP را از گوگل پلی، اپ‌استور یا پس‌کوچه دانلود کنید. وقتی که اپلیکیشن را نصب و باز کردید، دستورالعمل را دنبال کنید و دکمه‌ی اسلایدر را برای اتصال روشن کنید.

مزایا و ویژگی‌ها

این اپلیکیشن رایگان است و کار با آن بسیار ساده است. نسخه‌ی پولی آن نیز موجود است که سرعت اتصال شما را تا ۳۰٪ بالاتر می‌برد.
این اپلیکیشن به دست شرکت Cloud-flare تهیه شده است، نامی معتبر در زمینه‌ی امنیت وب‌سایت و اپلیکیشن که کارنامه بسیار درخشانی در حفظ امنیت داده‌های کاربران خود دارد. این شرکت دارای سیاست «ثبت نکردن داده» است و هیچگونه اطلاعات شخصی قابل شناسایی مربوط به استفاده شما از این اپلیکیشن را ذخیره نمی‌کند.
همچنین استفاده از این اپلیکیشن سبب میشود که سرویس‌دهنده اینترنت شما ن‌تواند داده‌های مربوط به الگوهای فعالیت شما را در اینترنت برای فروش به تبلیغ کنندگان، جمع‌آوری کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌ده

این اپلیکیشن به عنوان یک ابزار برای دور زدن طراحی نشده است، و بنابراین نباید انتظار داشت که به وب‌سایت‌های سانسور شده تحت هر شرایطی دسترسی ایجاد کند. بعضی از کاربران گزارش داده‌اند که استفاده از این اپلیکیشن برای باز کردن برخی وب‌سایت‌ها و اپلیکیشن‌ها مانند یوتیوب و گوگل پلی استور، چالش‌برانگیز بوده است.
همانطور که پیشتر اشاره شد، این اپلیکیشن تنها میزان محدودی امنیت حریم خصوصی فراهم می‌کند. هر چند که فعالیت‌های شما را از ISP مخفی نگه می‌دارد، اما IP شما را از وب‌سایت‌هایی که دیدن می‌کنید پنهان نمی‌کند.

Outline

Android | iOS | Windows | Linux

اوتلاین فرایند ساختن یک وی‌پی‌ان (VPN) را آسان‌تر و کم‌هزینه‌تر می‌کند و به شما اجازه می‌دهد تا آن را مدیریت کنید و کاربران را به سرور خودتان اضافه کنید. شما می‌توانید سرورهایی را روی آمازون، گوگل یا هر شرکت ارائه‌دهنده‌ی خدمات ابری دیگر قرار دهید. یکی از راه‌هایی که حکومت‌ها سرورهای وی‌پی‌ان را مسدود می‌کنند، از طریق تشخیص حجم بالای مصرف آنها است.

با این حال، با توجه به این‌که شما از طریق اوتلاین فقط از یک وی‌پی‌ان خصوصی برای خودتان و گروه محدودی استفاده می‌کنید، می‌تواند شناسایی‌شدن وی‌پی‌ان را بسیار دشوارتر کند.

سهولت استفاده

نرم‌افزار اوتلاین منیجر مناسب برای سیستم‌تان را نصب کنید و ارائه‌دهنده‌ی سرویس ابری خودتان را انتخاب کنید. پس از انتخاب آن، با فرایند آماده‌سازی خاص آن‌ها آشنا خواهید شد. شما می‌توانید سرورتان را از روی اوتلاین منیجر مدیریت کنید.

پس از تنظیم سرورتان، می‌توانید کلیدهای دسترسی یکتایی را مستقیماً از نرم‌افزار دسکتاپ منیجر ایجاد کنید. منیجر به شما امکان می‌دهد تا دعوت‌نامه‌هایی را از طریق پلتفرم ارتباطی دلخواه، برای اتصال به سرورتان بفرستید. کلیدهای دسترسی یعنی چگونه دستگاه‌هایتان را به اوتلاین منیجر وصل می‌کنید و با استفاده از سرورتان از آن‌ها محافظت می‌کنید. هر کلید دسترسی خاص و یکتاست و می‌تواند مستقیماً از روی سرور تنظیم یا حذف شود. محدودیت‌های داده، به شما امکان می‌دهد تا میزان پهنای باند مجاز برای هر کلید را کنترل کنید.

سپس، اپ اوتلاین کلاینت را دانلود کنید و با استفاده از کلید دسترسی خاص خودتان وصل شوید. اپ کلاینت نسخه‌هایی برای دسکتاپ و دستگاه‌های همراه دارد، بنابراین می‌توانید از هرجایی که باشید و از تمام دستگاه‌هایتان به اینترنت آزاد دسترسی پیدا کنید و به‌طور خصوصی با دیگران ارتباط برقرار کنید.

مزایا و ویژگی‌ها

از آنجا که وی‌پی‌انی که شما روی سرورتان اجرا می‌کنید فقط به وسیله‌ی شما و گروه محدودی مورد استفاده قرار می‌گیرد، شناسایی آن بسیار دشوارتر است و کارکردن با آن نیز باید خیلی ارزان‌تر باشد. اوتلاین همچنین می‌گوید که از یک «پروتکل بدون دست‌دادن و شبیه به هیچ‌چیز که شناسایی‌اش دشوار است» استفاده می‌کند، که باعث می‌شود کار مأموران حکومتی در تشخیص و مسدود کردن آن سخت‌تر شود.

در صورتی که سرور شما مسدود شود، باید به‌سادگی بتوانید یک سرور دیگر را با استفاده از همین روش از نو راه‌اندازی کنید.

این برنامه اطلاعات شخصی کاربران و اطلاعات وبسایت‌هایی که او مشاهده یا با آن‌ها ارتباط برقرار می‌کند را جمع‌آوری نمی‌کند. اطلاعاتی که این برنامه جمع‌آوری می‌کند را می‌توانید اینجا به تفصیل مطالعه کنید.

اوتلاین متن‌باز است،و در دو بررسی امنیتی مستقل تایید شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

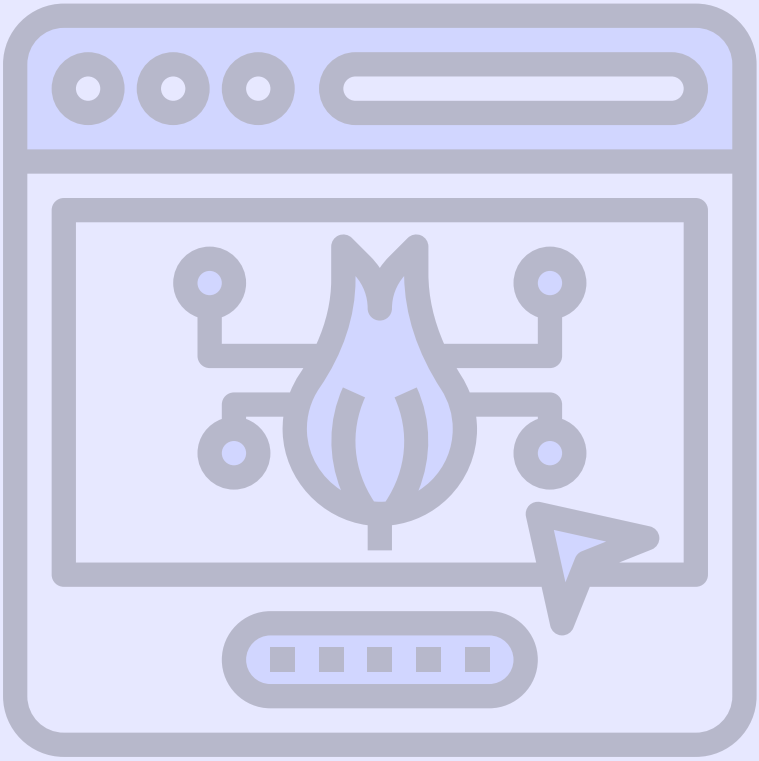
هر وی‌پی‌ان امنی به دسترسی به سرورهای بین‌المللی روی سرویس‌های ابری وابسته است و بنابراین در صورت قطعی کامل اینترنت، وی‌پی‌ان خصوصی شما کم‌وبیش قطعاً از کار خواهد افتاد، درست مانند هر وی‌پی‌ان تجاری دیگری که در بازار موجود است.

به صورت ناشناس از اینترنت استفاده کنید
اما انتظار پایین آمدن سرعت را داشته باشید

همانند وی‌پی‌ان‌ها، اپلیکیشن‌های فعال شده از سوی «تور» نیز در صورت انسداد پهنای باند به کار خود ادامه می‌دهند، با این حال سرعت پایین باز هم در خطر کندتر شدن قرار دارد. حتی در این حالت هم ما توصیه می‌کنیم که کار با «تور» را ادامه دهید تا اتصال خود را به صورت گمنام نگه دارید، به خصوص اگر با اطلاعات حساسی سروکار دارید.

در موقعیت‌هایی که اتصال «تور»، فیلتر می‌شود و یا انسداد پهنای باند به وجود می‌آید، می‌توانید استفاده از «Tor bridge» را جایگزین کنید. این پل‌ها، رله‌های Tor هستند که در فهرست اصلی «تور» درج نشده‌اند. از آنجایی که لیست کاملی از آن‌ها برای عموم وجود ندارد، حتی اگر ISP شما اتصال به تمام رله‌های شناخته شده «تور» را فیلتر کند، نمی‌تواند تمام پل‌ها را ببندند.

دوستان ما در پس‌کوچه یک معرفی عالی درباره کار با «تور» تهیه کرده‌اند که شامل توصیه‌هایی درباره وصل شدن به اینترنت از طریق پل‌های «تور» است.



Tor Browser

Android | MacOS | Windows | LINUX

مرورگر «تور» یک مرورگر متن‌باز است که با هدف حفظ حریم خصوصی شما در فضای آنلاین و همچنین عبور از فیلترها طراحی شده. روش کار آن به این صورت است که ترافیک شما را پیش از رسیدن به مقصد، حداقل بین سه گره‌ی اتصالی (سرورهای داوطلب) حرکت می‌دهد.

سهولت استفاده

مرورگر «تور» روی سیستم عامل ویندوز و MacOS و همچنین گوشی‌های همراه اندروید موجود است ولی هنوز روی دستگاه‌های iOS وجود ندارد. از طریق لینک‌های بالا می‌توانید آن را دانلود و نصب کنید.

نصب کردن مرورگر «تور» تا حدی از ابزارهای دیگری که در اینجا معرفی کرده‌ایم پیچیده‌تر است. وبسایت پس‌کوچه دستورالعمل نصب این اپلیکیشن را به صورت دقیق و با جزییات آماده کرده است که به شما کمک می‌کند تا وضعیت امنیتی و شبکه‌ی مورد استفاده خود را در ایران تنظیم کنید.

مزایا و ویژگی‌ها

«تور» شما را گمنام نگه داشته و اطمینان حاصل می‌کند که داده‌های شما از چشم سازمان‌های خصوصی و دولتی که بخواهند بر آن‌ها نظارت کنند، مخفی بماند. «تور» یک فناوری است که امتحان خود را پس داده و ثابت کرده که در این زمینه و همینطور در زمینه‌ی دور زدن فیلترها موثر عمل می‌کند.

همچنین استفاده از این اپلیکیشن سبب میشود که سرویس‌دهنده اینترنت شما نتواند داده‌های مربوط به الگوهای فعالیت شما را در اینترنت برای فروش به تبلیغ کنندگان، جمع‌آوری کند.

از نسخه ۱۱.۵ به بعد در این اپلیکیشن تمهیداتی برای دور زدن راحتتر فیلترینگ و سانسور در نظر گرفته شده است. این نسخه به طور خودکار و بر اساس موقعیت محلی شما، مناسبت‌ترین پل‌ها را برای دور زدن فیلترینگ انتخاب می‌کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

ایران تلاش زیادی برای فیلتر کردن «تور» داشته است و باعث شده که وصل شدن به اینترنت از ایران نسبت به کشورهای دیگر با چالش‌های بیشتری روبه‌رو باشد.همچنین باید توجه داشت که در هنگام استفاده از «تور» با پایین آمدن سرعت اینترنت مواجه خواهید شد.هر چند این اپلیکیشن در حفظ امنیت شما بی‌مانند است، اما این موضوع به قیمت پایین آمدن سرعت تمام می‌شود.

محتوای ترافیک شما به وسیله «تور»محافظت می‌شود اما برای ماموران حکومتی کار چندان سختی نیست که متوجه استفاده شما از «تور» بشوند.حواستان باشد که این موضوع می‌تواند فعالیت‌های شما را در معرض سوءظن قرار دهد.

OrBot

Android | iOS | F-Droid

«اوربوت» یک اپلیکیشن پروکسی رایگان است که کمک می‌کند اپلیکیشن‌های دیگر به شکل امن‌تری از اینترنت استفاده کنند. «اوربوت» از «تور» استفاده می‌کند تا ترافیک اینترنتی شما را رمزگذاری کند و سپس آن را به کامپیوترهای متعددی در نقاط مختلف دنیا می‌فرستد و از این طریق داده‌های ترافیک شما را مخفی نگه می‌دارد.

سهولت استفاده

می‌توانید نسخه‌ی اندروید این اپلیکیشن را از لینک‌های بالا دانلود کنید. برای بعضی مدل تلفن‌های گلکسی سامسونگ، چند مرحله‌ی اضافی وجود دارد تا این اپلیکیشن فعال شود. این مراحل در این ویدیو توضیح داده شده است.

مزایا و ویژگی‌ها

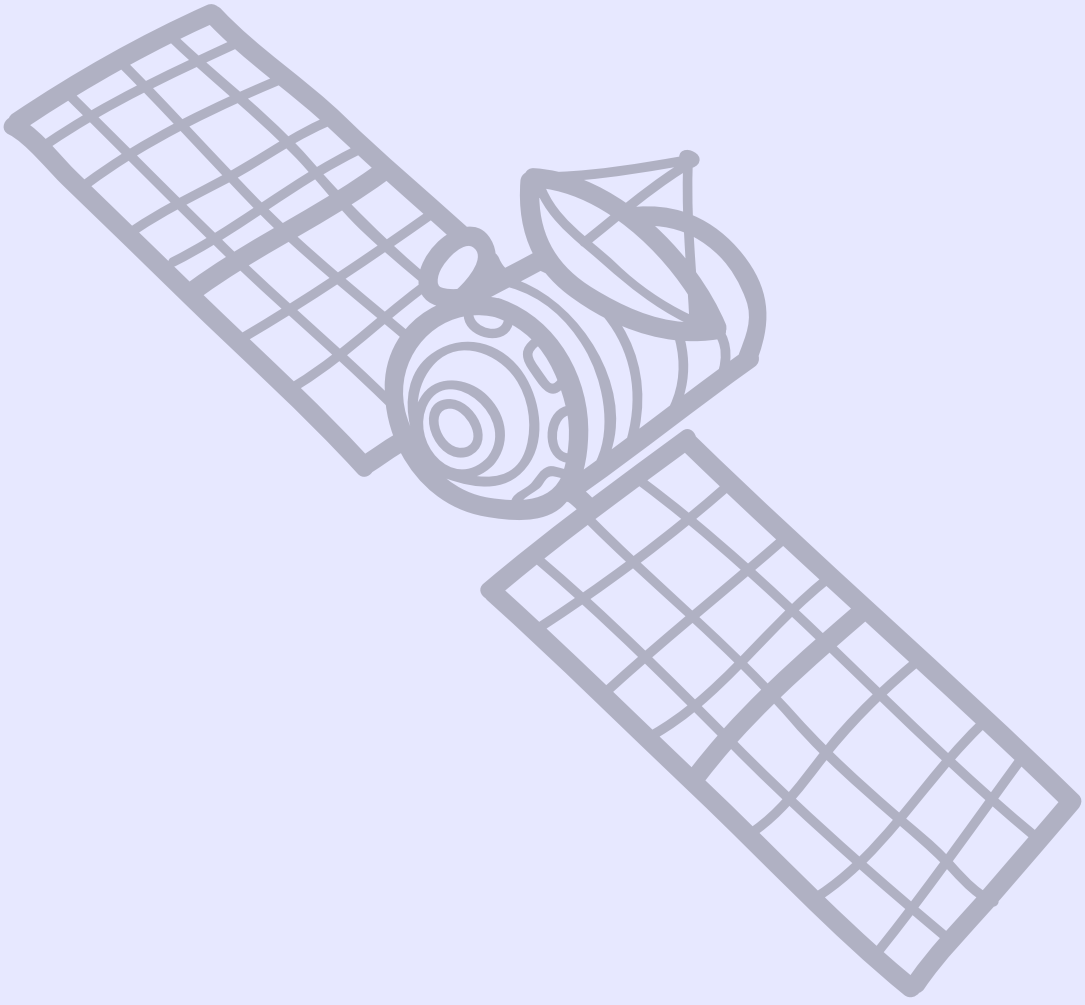
استفاده از «تور» می‌تواند شما را در برابر نظارت و شنود روزمره محافظت کند. زمانی که از «اوربوت» استفاده می‌کنید، ترافیک شما در حین گذشتن از شبکه‌ی «تور»، سه نوبت رله و رمزگذاری می‌شود، و به این وسیله یکی از قوی‌ترین روش‌های ممکن حفاظتی و گمنام ماندن در فضای آنلاین فراهم می‌گردد.
ویژگی دیگر این است که در داخل این اپلیکیشن، شما می‌توانید اپلیکیشن‌های دیگری را که می‌خواهید به دست «تور» محافظت شوند انتخاب کنید. این کار به این معنا است که سرعت اپلیکیشن‌ها و فعالیت‌های غیرحساس، بی‌دلیل پایین نخواهد آمد، مسئله‌ای که در مورد کار با «تور» از عوارض جانبی آن محسوب می‌شود.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

همانطور که در بالا اشاره شد، در برخی مدل‌های تلفن همراه لازم است که از چند مانع فنی اضافی برای فعال کردن این اپلیکیشن گذر کرد. همانند دیگر ابزارهایی که از طریق «تور» حفاظت می‌شوند، این اپلیکیشن نیز سرعت اتصال شما را پایین می‌آورد.
محتوای ترافیک شما به وسیله «تور» محافظت می‌شود اما برای ماموران حکومتی کار چندان سختی نیست که متوجه استفاده شما از «تور» بشوند. حواستان باشد که این موضوع می‌تواند فعالیت‌های شما را در معرض سوءظن قرار دهد.

پخش همگانی داده-
پخش‌های ماهواره‌ای، جایگزین بسیار خوبی هستند

اگر برقراری یک اتصال امن به اینترنت با اشکال پیش می‌رود و نگران این هستید که دسترسی خود را به اطلاعات از دست بدهید، شاید زمان خوبی باشد که به سرویس‌های ماهواره‌ای روی بیاورید. قبل از اینکه اختلال پیش بیاید باید سرویس ماهواره‌ای «توشه» را دانلود و نصب کنید.
«توشه» بر پایه فناوری پخش همگانی داده از طریق ماهواره عمل می‌کند، شما می‌توانید مستقیما از طریق ماهواره و روی تلویزیون خود به اخبار، فایل‌های تصویری و صوتی، و محتوای اینترنتی دسترسی پیدا کنید. راه‌اندازی آن کمی زمان‌بر است، اما اگر این کار را انجام دهید، در صورت اختلال در اینترنت یا قطع شدن آن، به هیچ‌وجه اتصال خود را به شکل کامل با دنیای بیرون از دست نخواهید داد.



Tooshe

Android | Windows | Linux

فناوری مورد استفاده در توشه این امکان را فراهم می‌کند که داده‌های غیر ویدیویی را به پخش زنده‌ی تلویزیونی تبدیل کند. داده‌ها دسته‌بندی می‌شوند، روی یک سرور بارگذاری می‌شوند، توسط ماهواره‌های موجود پخش می‌شوند و بعد توسط کاربران ضبط و رمزگشایی می‌شوند. این کار به کاربران این اجازه را می‌دهد تا در صورت قطع موقت و یا کامل اینترنت، به اخبار، اطلاعات و منابعی که از خارج از کشور فرستاده می‌شود دسترسی پیدا کنند

سهولت استفاده

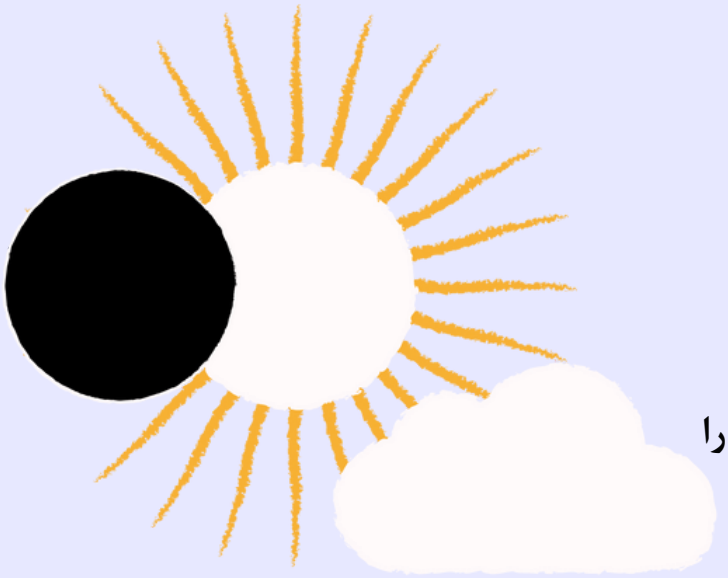
یک «یو-اس-بی فلش درایو» ساده که به دستگاه رسیور (گیرنده دیجیتال) وصل شده است، اطلاعات را ذخیره می‌کند، سپس کاربر فلش درایو را به یک تلفن همراه یا کامپیوتر وصل می‌کند و توسط نرم‌افزار رمزگشایی و مشاهده‌ی فایل «توشه» محتوا را به شکل اولیه‌ی آن مشاهده می‌کند.
اپلیکیشن توشه از مرداد ماه ۱۴۰۱ بر روی سیستم عامل لینوکس نیز قابل استفاده است.
راهنمای نصب و استفاده این اپلیکیشن رمزگشایی و مشاهده فایل را می‌توانید روی وب سایت «توشه» که در بالا لینک شده است پیدا کنید.
همچنین داده‌های توشه را می‌توانید از طریق: ماهواره: یاه سَت | فرکانس: ۱۱۷۶۶| سیمبل ریت: ۲۷۵۰۰ | پولاریزاسیون: عمودی، دریافت کنید.

مزایا و ویژگی‌ها

هر وقت در ایران یک اختلال اینترنتی بوجود می‌آید، «توشه» یک بسته‌ی روزانه به اشتراک می‌گذارد که شامل ابزارهای «پروکسی»، اپلیکیشن‌های پیام‌رسان رایج (به همراه بروزرسانی) ، آموزش امنیت دیجیتال، اپلیکیشن‌های اشتراک گذاری فایل، ابزارهای حریم خصوصی و بسته‌های مخصوص تظاهرات، می‌باشد.
فناوری پخش ماهواره‌ای داده‌ی «توشه» قادر است تا اطلاعات را در قالب‌های مختلف، و نه فقط ویدیو، پخش کند. پی‌دی‌اف، جی‌پگ، اچ‌تی‌ام‌ال، ام‌پی‌تری یا هر قالب دیگری که باشد، هنگامی که کاربر شبکه‌ی ماهواره‌ای را ضبط می‌کند، جمع‌آوری می‌شود.
فناوری «توشه» به وسیله برقراری ارتباط یک‌طرفه، به شکلی امن و بدون فاش شدن هویت افراد عمل می‌کند. از آنجایی که اطلاعات به همان شکل تلویزیون ماهواره‌ای به اشتراک گذاشته و دریافت می‌شود، محتوای مورد نظر کاربران قابل نظارت نخواهد بود و اطلاعات شخصی افراد هیچگاه جمع‌آوری و یا به اشتراک گذاشته نمی‌شود.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از «توشه» نمی‌توانید بنا به میل خود برای گشت‌زنی در اینترنت استفاده کنید، فقط این امکان را دارید تا محتوایی که توشه جمع‌آوری و پخش می‌کند را دانلود کنید.
از آنجایی که پخش اطلاعات به صورت یکطرفه انجام می‌شود، نمی‌توانید از توشه برای برقراری ارتباط با افراد دیگر و یا فرستادن فایل به خارج از کشور، استفاده کنید. کاربرد توشه عمدتاً ایجاد دسترسی به اطلاعات حیاتی در مواقع بحرانی می‌باشد.



جعبه ابزار قطع اینترنت

اعتراضات آبان ماه ۱۳۹۸ قطعی طولانی اینترنت را به همراه داشت که ایران را به مدت ده روز به خاموشی کامل اطلاعات فرو برد.این زمان برای بعضی استان‌های کشور مانند سیستان و بلوچستان و خوزستان حتی طولانی‌تر نیز بود. در طول این مدت، برقراری ارتباط با خانواده، دوستان و همکاران از طریق ابزارهای اینترنتی و یا دسترسی به وب‌سایت‌ها و اشتراک‌گذاری فایل‌ها، تقریباً غیرممکن شده بود.

قطع شدن‌های این چنینی به این منظور طراحی می‌شوند تا اخبار دستگیری‌ها، سرکوب‌ها و موارد نقض حقوق بشر پوشیده بماند. علاوه بر نقض حقوق اساسی ایرانیان، این اتفاقات صدمات بزرگی به اقتصاد و معیشت مردم وارد می‌کند.

قطعی‌های اینترنت بسیار چالش‌برانگیز هستند، با این حال می‌توان مقدماتی را فراهم آورد تا برای وقوع آن آماده بود و بدین صورت در زمانی که دسترسی به اینترنت وجود ندارد بتوانید با کانتکت‌های اصلی خود ارتباط برقرار کنید و به اطلاعات از خارج از کشور دسترسی بیابید.

جعبه‌ابزار ویژه‌ی قطع اینترنت که ما فراهم کرده‌ایم شامل راهنمایی درباره قدم‌هایی است که می‌توانید برای ایجاد آمادگی در برابر قطع اینترنت – شبیه اتفاقی که در آبان ماه ۱۳۹۸ افتاد – بردارید.

دسترسی به اطلاعات

دسترسی به اطلاعات در زمان قطعی اینترنت می‌تواند بسیار حیاتی باشد. درست است که رسانه‌های خارج از کشور می‌توانند از طریق ماهواره برنامه‌های خود را پخش کنند و شما را در جریان امور قرار دهند، اما در برخی مواقع ممکن است بخواهید به منابع تخصصی خاص دسترسی داشته باشید یا فایل‌هایی را استفاده کنید که قبل از قطعی اینترنت دانلود نکرده‌اید.
دو گزینه برای این شرایط در دسترس است: سرویس‌هایی مانند توشه که محتوای برگزیده اینترنتی را برای شما به صورت بسته‌های روزانه ارسال می‌کنند، یا ابزارهای آزمایشی مانند مرورگر همتا به همتای (peer-to-peer) CENO. در ادامه می‌توانید اطلاعات بیشتر برای هر کدام از این‌ها را به دست بیاورید.

ارسال داده‌ها از طریق ماهواره – راهی قابل‌اعتماد برای دسترسی به اطلاعات

قطع اینترنت می‌تواند تجربه‌ی بسیار ناراحت‌کننده‌ای باشد. نه تنها گپ‌زدن با دوستان و خانواده تقریباً غیرممکن می‌شود، بلکه ناگهان دسترسی به اطلاعات قابل‌اعتماد و درست درباره اتفاقاتی که دارد در سراسر کشور و جهان رخ می‌دهد نیز سخت‌تر می‌شود.
اینجا زمانی است که ابزار «توشه» به کار می‌آید. توشه به شما اجازه می‌دهد تا به وسیله‌ی همان بشقاب‌های ماهواره‌ای (دیش) که برای دیدن تلویزیون ماهواره‌ای استفاده می‌کنید، به اخبار، اطلاعات و منابع از خارج از کشور دسترسی پیدا کنید. در زمان قطع اینترنت، توشه معتبرترین راه ممکن برای با خبر ماندن از اتفاقات و دریافت توصیه‌هایی در زمینه حفظ امنیت در زمان بحران است.
این ابزار به کمی زمان برای نصب و راه‌اندازی نیاز دارد اما نکته‌ی مهم این است که دریافت اطلاعات از طریق توشه غیرقابل تشخیص است و حکومت آن را مانند دیدن تلویزیون ماهواره می‌پندارد و به همین دلیل یکی از امن‌ترین راه‌ها برای دسترسی به اطلاعات سانسور نشده است.

Tooshe

Android | Windows | Linux

فناوری مورد استفاده در توشه این امکان را فراهم می‌کند که داده‌های غیر ویدیویی را به پخش زنده‌ی تلویزیونی تبدیل کند. داده‌ها دسته‌بندی می‌شوند، روی یک سرور بارگذاری می‌شوند، توسط ماهواره‌های موجود پخش می‌شوند و بعد توسط کاربران ضبط و رمزگشایی می‌شوند. این کار به کاربران این اجازه را می‌دهد تا در صورت قطع موقت و یا کامل اینترنت، به اخبار، اطلاعات و منابعی که از خارج از کشور فرستاده می‌شود دسترسی پیدا کنند

سهولت استفاده

یک «یو-اس-بی فلش درایو» ساده که به دستگاه رسیور (گیرنده دیجیتال) وصل شده است، اطلاعات را ذخیره می‌کند، سپس کاربر فلش درایو را به یک تلفن همراه یا کامپیوتر وصل می‌کند و توسط نرم‌افزار رمزگشایی و مشاهده‌ی فایل «توشه» محتوا را به شکل اولیه‌ی آن مشاهده می‌کند.

اپلیکیشن توشه از مرداد ماه ۱۴۰۱ بر روی سیستم عامل لینوکس نیز قابل استفاده است.

راهنمای نصب و استفاده این اپلیکیشن رمزگشایی و مشاهده فایل را می‌توانید روی وب سایت «توشه» که در بالا لینک شده است پیدا کنید.

همچنین داده‌های توشه را می‌توانید از طریق: ماهواره: یاه سَت | فرکانس: ۱۱۷۶۶| سیمبل ریت: ۲۷۵۰۰ | پولاریزاسیون: عمودی، دریافت کنید.

مزایا و ویژگی‌ها

هر وقت در ایران یک اختلال اینترنتی بوجود می‌آید، «توشه» یک بسته‌ی روزانه به اشتراک می‌گذارد که شامل ابزارهای «پروکسی»، اپلیکیشن‌های پیام‌رسان رایج (به همراه بروزرسانی) ، آموزش امنیت دیجیتال، اپلیکیشن‌های اشتراک گذاری فایل، ابزارهای حریم خصوصی و بسته‌های مخصوص تظاهرات، می‌باشد.

فناوری پخش ماهواره‌ای داده‌ی «توشه» قادر است تا اطلاعات را در قالب‌های مختلف، و نه فقط ویدیو، پخش کند. پی‌دی‌اف، جی‌پگ، اچ‌تی‌ام‌ال، ام‌پی‌تری یا هر قالب دیگری که باشد، هنگامی که کاربر شبکه‌ی ماهواره‌ای را ضبط می‌کند، جمع‌آوری می‌شود.

فناوری «توشه» به وسیله برقراری ارتباط یک‌طرفه، به شکلی امن و بدون فاش شدن هویت افراد عمل می‌کند. از آنجایی که اطلاعات به همان شکل تلویزیون ماهواره‌ای به اشتراک گذاشته و دریافت می‌شود، محتوای مورد نظر کاربران قابل نظارت نخواهد بود و اطلاعات شخصی افراد هیچگاه جمع‌آوری و یا به اشتراک گذاشته نمی‌شود.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از «توشه» نمی‌توانید بنا به میل خود برای گشت‌زنی در اینترنت استفاده کنید، فقط این امکان را دارید تا محتوایی که توشه جمع‌آوری و پخش می‌کند را دانلود کنید.

از آنجایی که پخش اطلاعات به صورت یکطرفه انجام می‌شود، نمی‌توانید از توشه برای برقراری ارتباط با افراد دیگر و یا فرستادن فایل به خارج از کشور، استفاده کنید. کاربرد توشه عمدتاً ایجاد دسترسی به اطلاعات حیاتی در مواقع بحرانی می‌باشد.

استفاده از اینترنت از طریق فناوری peer-to-peer

تلویزیون ماهواره‌ای و ابزارهایی مانند توشه می‌توانند به شما کمک کنند تا در صورت قطعی اینترنت، همچنان از دنیای بیرون خبر بگیرید و به اطلاعات کلیدی دست پیدا کنید. اما، این روش‌ها راهکارهای مناسبی برای دسترسی به اینترنت جهانی نیستند.
ابزارهای در دست توسعه که به دسترس‌پذیرکردن بیشتر اطلاعات کمک می‌کنند اغلب در مرحله آزمون و خطا هستند، گرچه این ابزارها راه‌حل‌های جالبی ارائه می‌دهند. توسعه‌یافته‌ترین این ابزارها در حال حاضر مرورگر CENO است، که اصول همتا به همتا را روی مرورگری آنلاین پیاده می‌کند.
این اپ به کاربران امکان می‌دهد تا داده‌های زیاددیده‌شده را روی شبکه‌ای توزیع‌شده «ذخیره‌سازی» کنند. در صورتی که دسترسی به اینترنت جهانی قطع شود، کاربران می‌توانند به این داده‌های از پیش ذخیره‌شده دسترسی یابند، و در واقع نسخه‌هایی ذخیره‌شده از وب‌سایت‌ها را از سایر کاربران مرورگر CENO به شیوه‌ی «تورنت» دریافت کنند. این به معنای آن است که مرورگر CENO – به‌عنوان ابزاری برای دسترسی به اطلاعات در زمان قطعی اینترنت – هرچه کاربران بیشتری داشته باشد، قدرت بیشتری نیز خواهد داشت.

CENO Browser

Android | GitHub

مرورگر سِنو (کوتاه‌شده‌ی عبارت «نه به سانسور!»)، ساخت شرکت eQualitie است. یک مرورگر وب برای اندروید که به کاربران کمک می‌کند از طریق ارتباط‌هایی با میانجی پروکسی، یا از طریق محتوای پایداری از کاربران دیگر که در شبکه‌ی مرورگر ذخیره می‌شود، سانسور اینترنت را دور بزنند. این مرورگر در واقع نسخه‌ای سازگارشده از مرورگر پرطرفدار فایرفاکس است.

وقتی که یک کاربر با استفاده از این مرورگر به صفحه‌ای روی اینترنت دسترسی می‌یابد، مرورگر داده‌ها را روی شبکه ذخیره می‌کند و به سایر کاربران نیز امکان می‌دهد تا از طریق ارتباط‌های همتا به همتا به آن دسترسی پیدا کنند. به این ترتیب هر محتوای پرطرفداری حتی در زمان فیلترینگ سنگین، کُندشدن اینترنت، و یا حتی قطعی کامل اینترنت می‌تواند در دسترس کاربران این مرورگر باقی بماند.

سهولت استفاده

شما می‌توانید این نرم‌افزار را نصب کنید و از آن به‌عنوان یک مرورگر ساده‌ی اینترنت استفاده کنید، چون روی نسخه سازگارشده‌ای از مرورگر فایرفاکس برای اندروید ساخته شده است.

وقتی سعی می‌کنید با استفاده از مرورگر سنو صفحه‌ای را بارگذاری کنید، این اپ ابتدا سعی خواهد کرد تا مستقیماً یا با میانجی یک پروکسی به آن صفحه دسترسی پیدا کند. اما اگر نتواند از طریق این روش‌ها به صفحه‌ی مورد نظر دسترسی پیدا کند، «انبار مشترک» را جست‌وجو خواهد کرد تا ببیند آیا کاربر دیگری پیش از این به آن صفحه دسترسی یافته و آن را ذخیره کرده است. اگر این‌طور باشد، از این داده‌های ذخیره‌شده استفاده خواهد کرد تا صفحه را بارگذاری کند – روندی که می‌توان گفت شبیه «تورنت‌کردن» صفحه‌های وب از سایر کاربران مرورگر سنو است.

اگر این داده‌ها در شبکه وجود نداشته باشد، باز هم راه‌هایی برای دسترسی به آن‌ها از طریق «انژکتورها» دارید، که مانند میانجی‌ها یا پروکسی‌ها عمل می‌کنند و می‌توانند داده‌ها را به درون شبکه‌ی شما منتقل کنند.

علاوه بر این، مرورگر سنو دو شیوه برای مرور وب در اختیار شما می‌گذارد: عمومی و خصوصی. در «حالت عمومی» مرورگرتان سعی خواهد کرد تا به محتوای ذخیره‌شده از شبکه دسترسی پیدا کند، در حالی که در «حالت خصوصی» شما هرگز از داده‌های ذخیره‌شده استفاده نخواهید کرد و فقط مرورگر سنو را به‌عنوان یک پروکسی یا میانجی به کار خواهید برد.

مزایا و ویژگی‌ها

در صورت قطعی اینترنت، یا دوره‌ای از اختلال پایدار، استفاده از مرورگر سنو توانایی دسترسی به هر محتوای مهم یا پرطرفداری را که سایر کاربران سنو ذخیره‌شان کرده باشند، به کاربران می‌دهد. این مرورگر از این جهت بی‌همتاست که در صورت قطعی اینترنت، چنین امکاناتی را ارائه می‌دهد. هرگونه محتوای پرطرفداری روی شبکه ذخیره می‌شود و نمی‌تواند به‌زور حذف شود.

وقتی تعداد کافی از کاربران این داده‌ها را ذخیره کنند، این سیستم می‌تواند سرعت مرور بیشتری را در پی داشته باشد. از آنجا که مشترک شما می‌تواند بخش‌های مختلفی از یک محتوا را همزمان از مشترکان مختلفی دریافت کند، بارگذاری محتوای ارائه‌شده بین شبکه‌ها و دستگاه‌های مختلف تقسیم می‌شود. باز هم تکرار می‌کنیم: می‌تواند قیاس مفیدی باشد که این فرایند را مانند دریافت تکه‌تکه‌ی صفحه‌های اینترنتی پرطرفدار به شیوه‌ی «تورنت» از سایر کاربران مرورگر سنو تصور کنید.

مرورگر سنو می‌تواند امکان مرور ارزان‌تر را نیز فراهم کند. داده‌های ذخیره‌شده روی این شبکه به‌جای اینترنت بین‌المللی از طریق ارتباط‌های محلی در دسترس خواهند بود، یعنی شما برای دسترسی به محتوای «محلی» هزینه‌ی کمتری برای داده‌ها پرداخت می‌کنید، حتی وقتی این محتوا در اصل از اینترنت جهانی گرفته شده باشد.
آخرین نسخه این مرورگر شامل تغییراتی برای دسترسی بهتر به وب‌سایت‌هاست و همچنین امکان اضافه کردن سرورهای بوت‌استرپ «بیت‌تورنت» در تنظیمات برای به‌خاطرسپاری در راه‌اندازی‌های مجدد در آن تعبیه شده و تشخیص تغییرات در اتصال و راه اندازی مجدد «وی‌نت» به‌طور خودکار برای انطباق با محیط جدید نیز از دیگر امکانات نسخه ۱.۶.۱که در تیرماه ۱۴۰۱ عرضه شده می‌باشد.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

این اپ کاملا بی‌خطر نیست. اگرچه اطلاعات شخصی شما امن خواهند بود، احتمالاً هر فردی که آشنایی کاملی با سازوکار کوئینت داشته باشد می‌تواند ابزاری را توسعه دهد که نشان بدهد یک محتوای خاص از چه آدرس‌های آی‌پی به اشتراک گذاشته شده است. با این حال، این امکان وجود نخواهد داشت که آدرس آی‌پی یک کاربر مشخص هدف قرار گیرد و لیستی از تمام محتوایی که او ثبت کرده، به دست آید. با این همه، این اپ شاید برای کاربرانی که فعالیت‌های آنلاین‌شان نیازمند گمنامی کامل است، مناسب نباشد.
به طور کلی، اگر یک سایت خاص (مثلاً یک سایت دولتی) از شما می‌خواهد تا به‌عنوان فردی قابل‌شناسایی به آن وصل شوید، از یک منطقه‌ی مشخص، یا از طریق اینترنت ملی، تیم سازنده‌ی مرورگر سنو به شما توصیه می‌کنند که در این مورد در عوض از یک مرورگر وب معمولی استفاده کنید.
همچنین، تا وقتی کاربران بیشتری مرورگر سنو را دانلود و شروع به استفاده از آن کنند، احتمالاً مقدار نسبتاً محدودی از داده‌های ذخیره‌شده در شبکه وجود خواهد داشت. درست مانند هر فناوری همتا به همتا، مرورگر سنو نیز وقتی کارآمدتر خواهد شد که افراد بیشتری از آن استفاده کنند. تا زمانی که زیربنای کاربری آن تا حدی رشد نکند، شاید این راه هنوز کاملاً برای دسترسی به اطلاعات در زمان قطعی کامل اینترنت قابل‌اتکا نباشد.

اپلیکیشن‌های پیام‌رسان – برقراری ارتباط در خاموشی

زمانی که دسترسی به اینترنت جهانی بسته شده است، خیلی از اپلیکیشن‌های پیام‌رسانی که هر روز استفاده می‌کنید دیگر کار نخواهند کرد. اپلیکیشن‌هایی مانند «سیگنال»، «تلگرام» یا «واتس‌اپ» نیازمند دسترسی به سرورهای موجود در اینترنت جهانی هستند بنابراین در زمان قطع اینترنت به هیچ‌وجه موثر عمل نخواهند کرد.
باید به این موضوع توجه داشت که تمام ابزارهای برقراری ارتباط دیجیتال تا حدی دارای خطراتی هستند، و هیچ‌وقت نباید هنگام فرستادن اطلاعات حساس به دوستان، خانواده یا کانتکت‌هایتان، بی‌خیال امنیت بشوید– به خصوص در زمان قطعی اینترنت که تنش زیادی وجود دارد.
هر چند اپلیکیشن‌های زیر احتمالا در زمان قطع اینترنت به شما کمک می‌کنند، بعضی از آن‌ها دارای ضعف‌هایی هستند که باید به آنها توجه داشت.
یک نکته‌ی مهم: حتی اگر اپلیکیشن‌های پیام‌رسان داخلی در زمان قطع اینترنت در دسترس باشند، هیچ وقت نباید از آن‌ها استفاده کنید. بسیاری از این اپلیکیشن‌های داخلی روی شبکه ملی اطلاعات کار می‌کنند و به همین دلیل می‌توانند در زمان قطع اینترنت به کار خود ادامه بدهند. به هر حال بسیاری از آن‌ها دارای نقص‌های امنیتی هستند و هیچگونه حفاظت معناداری از داده‌های کاربران ارائه نمی‌دهند. هر داده‌ی حساسی که با اپلیکیشن‌های داخلی به اشتراک گذاشته شود، به راحتی قابل رهگیری و نظارت است.
پس چه گزینه‌هایی وجود دارد؟

استفاده از پیام رمزنگاری شده

اپلیکیشن پیام‌رسان «جمی» یکی دیگر از اپلیکیشن‌های همتا به همتا و سرتاسر رمزگذاری شده است که ممکن است در زمان قطع شدن اینترنت موثر عمل کند. هر چند مانند «برایر» دارای قابلیت بلوتوثی نیست، اما به شما اجازه می‌دهد تا از طریق شبکه‌های داخلی و محلی به آن وصل شوید.
روشن نیست که «جمی» چطور می‌تواند با شبکه‌ی ملی اطلاعات (اینترنت ملی) تعامل داشته باشد – ممکن است (ثابت نشده) برقراری ارتباط بین کاربران «جمی» با بهره‌برداری از اتصالات شبکه ملی اطلاعات، انجام‌پذیر باشد.
عدم قطعیت با وجود این موضوع بیشتر می‌شود که این اپلیکیشن برای شروع نیازمند دسترسی به یک سرور bootstrap است که این سرور به حفظ اتصال کمک می‌کند. این سرورهای bootstrap معمولاً روی اینترنت جهانی مستقر هستند، پس می‌شود انتظار داشت که در زمان قطع اینترنت و عدم دسترسی به یک bootstrap.، «جمی» با چالش‌هایی برای حفظ اتصال روبه‌رو شود.
البته در حرف این اپلیکیشن اظهار کرده است که کاربران دیگر می‌توانند به عنوان bootstrap عمل کنند (هر چند صحت این موضوع معلوم نیست) و یا یک سرور bootstrap روی یک سرور داخلی سوار شود (هر چند این موضوع خودش مسائل امنیتی متعددی را در بر خواهد داشت). به صورت خلاصه، «جمی» ممکن است موفق عمل کند، اما سوالات بدون پاسخ بسیاری وجود دارد.

Jami

Android | iOS | Windows | Linux

«جمی» پلتفرم رایگان برای ارتباط و مکاتبه است که ادعا می‌کند هویت و حریم خصوصی کاربران خود را حفاظت می‌کند. «جمی» دارای رمزگذاری سرتاسری است و به شکل همتا به همتا عمل می‌کند، بنابراین نیازی به یک سرور مرکزی برای انتقال داده بین کاربران ندارد.
به همین سبب، کاربرانی که روی یک شبکه‌ی محلی مشترک هستند (برای مثال، یک شبکه وای‌فای عمومی بدون دسترسی به اینترنت) باید بتوانند از طریق «جمی» به هم متصل شوند، حتی اگر به اینترنت وصل نباشند.

سهولت استفاده

دانلود این اپلیکیشن برای اندروید از گوگل‌پلی، و برای iOS از اپل استور امکانپذیر است. نسخه‌های مخصوص دسکتاپ (مک، ویندوز و لینوکس) را هم می‌توان از خود وبسایت «جمی» دانلود کرد.
برای ایجاد حساب جمی نیازی به ارائه هیچ مشخصات فردی و یا حتی شماره تلفن نیست.

مزایا و ویژگی‌ها

علاوه بر برقراری ارتباط امن، «جمی» تماس‌های ویدویی و کنفرانسی با کیفیت اچ‌دی را نیز ارائه می‌کند، اما کیفیت این تماس‌ها بسیار بستگی به کیفیت اینترنت مورد استفاده دارد.
داشتن قابلیت ارسال پیام از طریق شبکه‌های وای‌فای می‌تواند در زمان‌های قطع موقت اینترنت (و حتی قطع کامل اینترنت) به منظور برقراری ارتباط با کانتکت‌هایی که در نزدیکی شما هستند، موثر عمل کند. «جمی» همچنین ممکن است بتواند در صورت محدود شدن دسترسی به اینترنت جهانی به شکلی مطمئن عمل کند، اما تنها در صورتی که اینترنت ملی در دسترس باقی بماند.
به این موضوع توجه داشته باشید که محققان ما به صورت مستقل قادر به تایید این گزارش‌ها نبوده‌اند، بنابراین نمی‌توانند درباره کارکرد این اپلیکیشن در چنین شرایطی با قطعیت نظر بدهند. آزمایش‌ها و شواهد بیشتری برای این کار نیاز است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

بر خلاف برخی از اپلیکیشن‌هایی که بر پایه‌ی شبکه توری meshnet-based طراحی می‌شوند، «جمی» قادر به استفاده از بلوتوث برای برقراری ارتباط با دستگاه‌های دیگر نیست. برقراری ارتباط آفلاین با کانتکت‌ها، نیازمند اتصال هر دو طرف به یک شبکه‌ی اینترنت مشترک محلی است.
همچنین سازندگان راهی برای درخواست از بین بردن کامل اطلاعات در این اپلیکیشن در نظر نگرفته‌اند.

Nahoft

Android

«نهفت» که در فارسی به معنی پنهان است، یک نرم‌افزار آفلاین رمزنگاری پیام و حفظ حریم‌خصوصی برای استفاده در شبکه‌های ناامن است. در واقع «نهفت» یک پیام‌رسان نیست اما با رمزنگاری پیام‌ها، دسترسی دیگران به محتوای رد و بدل شده توسط شما و دوستان‌تان در دیگر پیام‌رسان‌ها را غیر ممکن می‌کند.
این برنامه توسط گروه حقوق بشری اتحاد برای ایران و در قالب پروژه‌ی ایران کوباتور ۲ توسعه داده شده است. سازمان اتحاد برای ایران یک نهاد حقوق بشری است که مرکز آن در شهر برکلی، ایالت کالیفرنیا قرار دارد. هدف این نهاد گسترش آزادی‌های مدنی در ایران، دفاع از حقوق بشر، حمایت از جامعه مدنی و ترغیب به مشارکت از طریق فناوری است.

سهولت استفاده

این نرم افزار متن باز که با تکنیک پنهان‌نگاری (Steganography) طراحی شده، کاملا آفلاین است و از هیچ سروری جهت ارسال یا دریافت یا رمزگذاری پیام‌های شما استفاده نمی‌کند.
شما می‌توانید متن خود را رمزگذاری کنید و آن را از طریق متن، کلمات شانسی یا انتخاب یک تصویر از گالری دستگاه خودتان ارسال کنید.
شما همچنین می‌توانید یک پیام را رمزگذاری کنید، آنرا در یک تصویر بگنجانید و در حافظه دستگاه خود نگهداری کنید.
در عین حال این امکان وجود دارد که پس از رمزگشایی و خواندن پیام دریافتی آن را در نهفت ذخیره کنید و یا در همان لحظه آن را پاک کنید.
همچنین این برنامه دارای قابلیت تعریف یک کد ورود تخریبی است. ایجاد این کد به شما کمک میکند که در زمان اضطرار و هنگامی که احتمال دسترسی دیگران به گوشی تلفن همراه شما ممکن است از آن استفاده کرده و تمام اطلاعات ذخیره شده در این نرم افزار را در یک لحظه پاک کنید.
نهفت در دو مرحله توسط پژوهشگران و متخصصان Cure۵۳ ارزیابی امنیتی شده و پیش از انتشار آخرین نسخه، پیشنهادات آنان برای بهبود امنیت اپ به کار گرفته شده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از آنجایی که اصولا فرآیند رمزنگاری فرآیند پیچیده‌ای است ممکن است استفاده از این برنامه برای تمام کاربران ساده نباشد. همچنین برخی کاربران از پیچیده بودن رابط کاربری این برنامه گلایه کرده‌اند.
این برنامه تا کنون تنها برای سیستم عامل اندروید طراحی شده و نسخه‌ای برای اپل، ویندوز و لینوکس ارائه نکرده است.

برقراری ارتباط مستقیم - اپلیکیشن‌های پیام‌رسان همتا به همتا peer-to-peer

راه حل جایگزین این است که از ابزارهای همتا به همتا و فناوری شبکه توری استفاده کنید. برخی از این نوع اپلیکیشن‌ها می‌توانند از طریق شبکه‌های وای‌فای محلی، بلوتوث یا حتی خود شبکه ملی اطلاعات، پیام‌های شما را ارسال کنند.
یکی از ابزارهایی که چنین برقراری ارتباطی را میسر می‌سازد «برایر» است. این ابزار از فناوری همتا به همتا استفاده می‌کند تا پیام‌های شما را از طریق بلوتوث یا وای‌فای همگام‌سازی کند.

Briar

Android | F-Droid app

««برایر» یک اپلیکیشن پیام‌رسان است که برای استفاده کنشگران، روزنامه‌نگاران و هر کس دیگری که احتیاج به برقراری ارتباط در زمان قطع اینترنت داشته باشد، طراحی شده است. برخلاف اپلیکیشن‌های پیام‌رسان سنتی، «برایر» متکی بر یک سرور مرکزی نیست، پیام‌ها با استفاده از یک شبکه توری به صورت مستقیم بین دستگاه‌های کاربران همزمان‌سازی یا همان synchronized می‌شوند.

سهولت استفاده

کاربران می‌توانند «برایر» را برای اندروید از پلی استور گوگل، F-Droid یا وب سایت برایر دانلود نمایند..

مزایا و ویژگی‌ها

«برایر» می‌تواند برای به اشتراک گذاشتن پیام‌های مهم با افرادی که به آن‌ها اعتماد دارید، به شکلی مطمئن عمل کند. در هنگام قطع شدن اینترنت، این اپلیکیشن اجازه می‌دهد تا داده‌ها و اطلاعات را با لیست مخاطبان(کانتکت‌ها) خود به شکلی امن به اشتراک بگذارید، البته لازم خواهید داشت تا با فرد گیرنده در محدوده‌ی بلوتوث یا روی یک شبکه وای‌فای مشترک قرار داشته باشید.

علاوه بر قابلیت گپ زدن سرتاسری خصوصی و گروهی، «برایر» به شما این امکان را می‌دهد تا تالارهای گفتگوی عمومی و بلاگ‌هایی تشکیل دهید که برقراری ارتباط را با گروه‌های معتمد میسر می‌سازد، و حتی در زمان‌های قطع اینترنت هم قابل اشتراک‌گذاری و به‌روزرسانی هستند.

تالارهای گفتگو، مکالمات غیر خصوصی هستند. بر خلاف گروه‌های خصوصی، هر کسی که به آن بپیوندد می‌تواند کانتکت‌های دیگر خود را به تالار دعوت کند. در ضمن بلاگ‌ها امکان پست و به اشتراک گذاشتن اخبار و بروزرسانی‌ها را با تمام کانتکت‌هایتان امکان پذیر می‌سازند.

«برایر» همچنین با اپلیکیشن "دکمه هشدار" Ripple مجهز شده است که می‌تواند برایر را مخفی کند یا در حالتی که نگران هستید حساب کاربری شما تحت نظارت قرار گرفته یا مصادره شده، می‌تواند طوری پیکربندی شود که حساب کاربری و تاریخچه پیغام‌های شما را پاک کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

این اپلیکیشن البته اشکالاتی نیز دارد. گزارش‌هایی از مشکلات برقراری ارتباط از طریق بلوتوث در زمانی که اینترنت قطع شده است دریافت شده، اما گروه «برایر» مشغول رفع این اشکالات هستند.

در زمان قطع اینترنت، این اپلیکیشن تنها در صورتی که کاربران در محدوده بلوتوث و وای‌فای یکدیگر قرار داشته باشند، می‌تواند کارایی داشته باشد.

مشکل دیگر این اپلیکیشن این است که تا زمانی که تعداد زیادی از افراد شروع به استفاده از «برایر» نکنند، نمی‌تواند در زمان‌های قطع دسترسی به اینترنت از تمام امکانات بالقوه خود استفاده کند و موثر واقع شود. برای اینکه «برایر» بتواند به یک اپلیکیشن پیام‌رسان قدرتمند تبدیل شود و جایگزین پیام‌رسان‌های معمول بشود، می‌بایست تعداد کاربران گسترده‌ای را جذب کند.

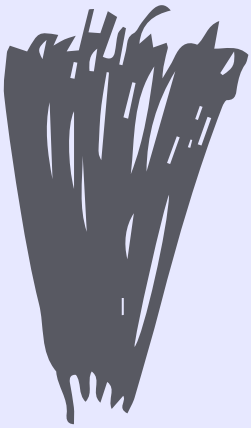
اطلاعیه‌ای در مورد اپلیکیشن «بریجفای»

در نسخه پیشین ایران در خاموشی، اپلیکیشن پیام‌رسان «بریجفای» که از فناوری بلوتوث استفاده می‌کند را معرفی کرده بودیم. با توجه به آسیب‌پذیری‌های امنیتی این اپلیکیشن، تصمیم گرفتیم آن را از جعبه ابزار ایران در خاموشی حذف کنیم. در حال حاضر استفاده از اپلیکیشن «بریجفای» را به عنوان یک اپلیکیشن پیام‌رسان امن توصیه نمی‌کنیم.

این اپلیکیشن در اصل برای کمک به حفظ ارتباط افراد در جاهایی مثل کنسرت یا سایر رویدادهای عمومی که ممکن است اینترنت دچار اختلال شود طراحی شده، اما برخی از تظاهرات کنندگان نیز از این اپ استفاده کرده‌اند، مثلا در شلوغی‌های سال ۲۰۱۹ – ۲۰۲۰ در هنگ‌کنگ و در مواقع قطعی اینترنت در میانمار.

اما این اپلیکیشن برای استفاده در تظاهرات طراحی نشده است و استفاده از آن در این رویدادها می‌تواند با خطرات جدی همراه باشد. در سال ۲۰۲۰ گروهی از محققان در مقاله‌ای در وبسایت اخبار فناوری Ars Technica از یک سری حفره‌های جدی امنیتی این اپلیکیشن انتقاد کردند. هرچند در اکتبر ۲۰۲۰ «بریجفای» یک نسخه جدید منتشر کرد، اما هنوز حسابرسی امنیتی مستقلی برطرف شدن این حفره‌های امنیتی را تایید نکرده است.

تا زمانی که «بریجفای» حسابرسی امنیتی مستقلی را با موفقیت نگذرانده است، توصیه می‌کنیم که در زمان قطعی اینترنت از استفاده از این اپلیکیشن جدا خودداری کنید. در صورت استفاده، حریم خصوصی و امنیتی خود را به خطر می‌اندازید.



آیا می‌توان از شبکه ایمیل بهره‌برداری کرد؟

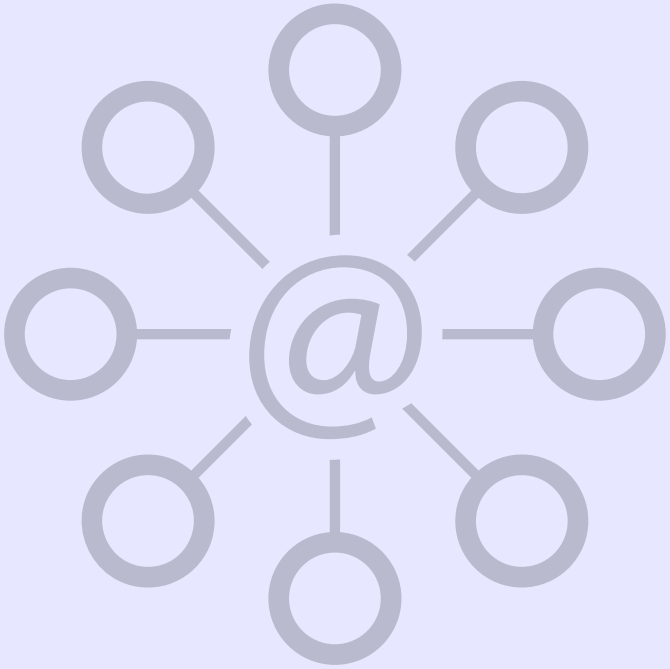
علاوه بر جامی، اپ پیام‌رسان دِلتاچت می‌تواند راه دیگری را برای برقراری ارتباط امن‌تر روی شبکه‌ی اطلاعات ملی فراهم کند. این اپ پیام‌رسان رمزگذاری‌شده، از شبکه‌های سرور ایمیل برای رساندن پیام‌ها به سایر کاربران دلتاچت استفاده می‌کند.

در نتیجه، اگر شما از یک سرویس ایمیل داخل ایران استفاده کنید که از طریق شبکه‌ی ملی اطلاعات کار می‌کند، این شانس وجود دارد که بتوانید در صورت محدود شدن دسترسی به اینترنت جهانی، همچنان با سایر کاربران دلتاچت پیام رد و بدل کنید.

با این حال، خیلی از ابزارهایی که وعده می‌دهند در زمان قطعی اینترنت کار کنند، مشکلاتی دارند – چه به‌لحاظ امنیتی و چه به‌لحاظ کاربردی.

اگرچه دلتاچت راهی برای فرستادن ایمیل‌های رمزگذاری‌شده روی شبکه‌ی ملی اطلاعات به افرادی که با آن‌ها در تماسید در اختیارتان می‌گذارد، روش رمزگذاری آن نقاط ضعف شناخته‌شده‌ای دارد و یک سرویس ارائه‌دهنده‌ی اینترنتی یا ایمیل پیگیر می‌تواند به فراداده‌های مرتبط با هویت کسانی که با آن‌ها در تماسید، دسترسی پیدا کنند و – حتی در موارد خاص – امکان دارد هویت افراد مورد تماس‌تان را جعل کنند و تماس‌هایتان را شنود کنند.

این اپ قطعاً می‌تواند تحت شرایط مناسب کارآمد باشد، اما لطفاً مطمئن شوید که پیش از استفاده از آن، به خطرهای احتمالی‌اش آگاهید.



Delta Chat

Android | F-Droid | iOS | Windows | Linux | macOS

دلتاچت یک پلتفرم رایگان و متن‌باز پیام‌رسان است. دلتاچت از شبکه‌های سرور ایمیل موجود استفاده می‌کند تا پیام‌های رمزگذاری‌شده‌ی سرتاسری را به سایر کاربران دلتاچت برساند. دلتاچت برای برقراری ارتباط رمزگذاری‌شده‌ی سرتاسری با سایر کاربران دلتاچت، از پروتکل رمزگذاری خودکار و سایر اپ‌های ایمیل سازگار با رمزگذاری خودکار استفاده می‌کند.

سهولت استفاده

کاربران می‌توانند نسخه‌ی اندروید این نرم‌افزار را از فروشگاه گوگل‌پلی و نسخه‌ی iOS را از اپ‌استور اپل دانلود کنند. نسخه‌های دسکتاپ (مک، ویندوز و لینوکس) نیز روی وب‌سایت دلتاچت در دسترس هستند.

مزایا و ویژگی‌ها

دلتاچت باید بتواند امکان برقراری ارتباط رمزگذاری‌شده روی شبکه‌ی ملی اطلاعات ایران را فراهم کند. از آنجا که دلتاچت از شبکه‌های سرور ایمیل استفاده می‌کند، در زمان قطعی محدود اینترنت، کاربران می‌توانند از سرویس‌های ارائه‌دهنده‌ی ایمیل داخل کشور برای فرستادن پیام‌های رمزگذاری‌شده استفاده کنند.

دلتاچت همچنین از پیام‌های حذف‌شونده پشتیبانی می‌کند، و کاربران می‌توانند صدا، تصاویر و فایل‌های کوچک‌تر از ۲۵ مگابایت را نیز ارسال کنند.

همچنین این برنامه از نسخه ۱.۳ به بعد با پیشتیبانی از اپ‌های webxdc به اشتراک گذاری فایل‌های HTML۵ را به قابلیت‌های خود افزوده است.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

پیام‌ها به‌طور خودکار رمزگذاری نمی‌شوند، مگر آن‌که گیرنده‌ی پیام‌تان هم از دلتاچت استفاده کند. اما حتی در این صورت هم، پروتکل رمزگذاری مبتنی بر رمزگذاری خودکار می‌تواند پیام‌های شما را از سوی شرکت ارائه‌دهنده‌ی سرویس ایمیل یا اینترنت‌تان، در معرض شنود قرار دهد.

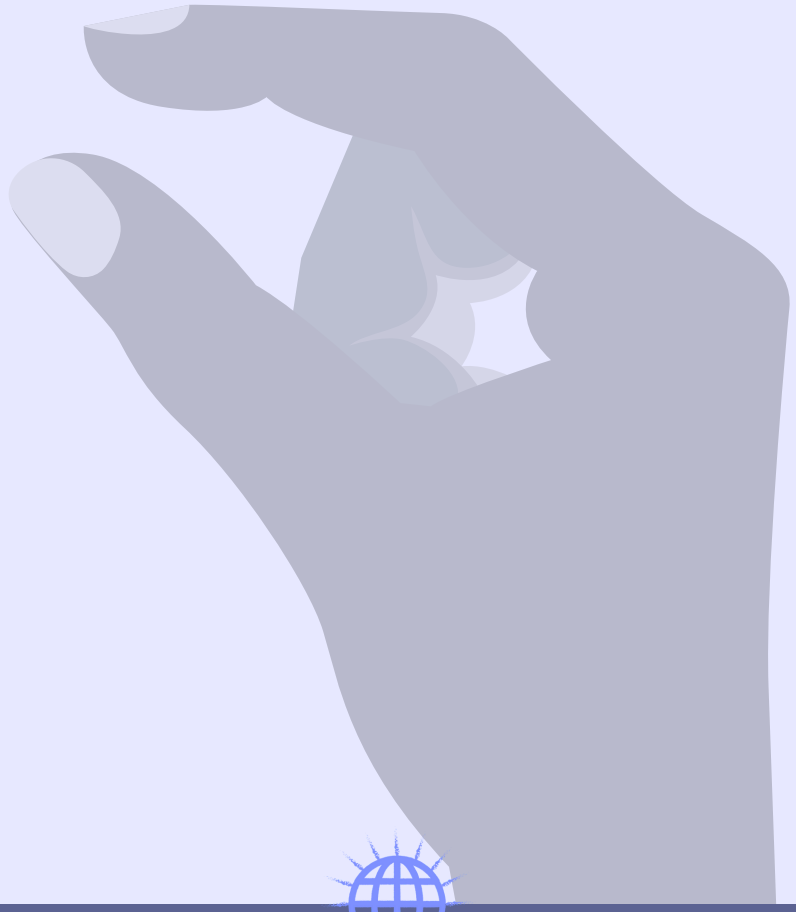
توجه کنید که استفاده از ایمیل‌های رمزگذاری‌شده در سرویس‌های ارائه‌دهنده‌ی ایمیل ملی می‌تواند برای این‌گونه شرکت‌ها کافی باشد تا کاربران را به اتهام فعالیت‌های مشکوک شناسایی و نشانه‌گذاری کنند. اگرچه، استفاده طیف گسترده‌تر کاربران از سرویس‌های ایمیل رمزگذاری‌شده، شناسایی کاربران مشخص به‌عنوان کاربر مشکوک را برای این سرویس‌ها دشوارتر می‌سازد، در حال حاضر این خطر را نمی‌توان نادیده گرفت.

به‌لحاظ نظری، برای شرکت‌های ارائه‌دهنده‌ی خدمات، کار ساده‌ای است که عنوان پیام‌ها را تحلیل کنند، و ترافیک رمزگذاری را کاهش دهند یا مسدود کنند، اگرچه تا به حال هیچ نمونه‌ی مستندی از چنین رویدادی گزارش نشده است.

بسیاری از شرکت‌های ارائه‌دهنده‌ی ایمیل ایرانی، برای ایجاد حساب کاربری نیازمند تصدیق هویت اضافی مانند ارائه‌ی شماره‌ی تلفن هستند، که اگر شما بخواهید یک حساب کاربری ایمیل «یک‌بارمصرف» گمنام در یک سرویس ایمیل بومی برای خودتان بسازید، می‌تواند چالش‌هایی را پیش بکشد. با این حال، کاربرانی که از سرور ایمیل داخل کشور خودشان استفاده می‌کنند، می‌توانند آسان‌تر از دلتاچت برای فرستادن پیام‌های رمزگذاری‌شده‌ی سرتاسری امن به دوستان و آشنایان‌شان استفاده کنند.

ابزارهای دور زدن – گزینه‌هایی محدود

در زمان قطع شدن اینترنت، اکثر وی‌پی‌ان‌ها و ابزارهای دور زدن بی‌فایده خواهند بود. وی‌پی‌ان‌های معمول شما را از طریق شبکه‌های همیشگی به وب‌سایت‌های اینترنت جهانی وصل می‌کنند. این بدین معنی است که وقتی اتصال به این شبکه‌ها مختل می‌شود، اتصال وی‌پی‌ان ها نیز دچار اختلالاتی می‌گردد.
از آنجایی که وی‌پی‌ان‌ها نیازمند دسترسی به سرورهای جهانی هستند، نمی‌توانند کمک چندانی برای شما باشند، حتی اگر شبکه ملی اطلاعات همچنان آنلاین مانده باشد.
تنها ابزار دور زدن که ادعا کرده است در آبان ۱۳۹۸ ایرانیان را به اینترنت جهانی متصل نگه داشته، اپلیکیشن «سایفون» است. سایفون از اقدامات متعدد و انطباق‌پذیری استفاده می‌کند تا فیلترها را دور بزند، و طبق گزارش‌ها قادر بوده تا از شکاف‌های موجود در اجرای پروژه قطع اینترنت ایران بهره‌برداری کرده و برخی کاربران را به اینترنت جهانی متصل نگه دارد.
البته در این موارد هم اتصال با سرعت پایین بوده و قابل اتکا نبوده است. همچنین نباید فراموش کنیم که «سایفون» گمنام ماندن کاربران و فاش نشدن هویتشان را فراهم نمی‌کند، پس زمانی که می‌خواهید به اطلاعات حساس دسترسی بیابید، باید با احتیاط از این اپلیکیشن استفاده کنید.



Psiphon

Android | iOS | Windows | Android direct source

««سایفون» ابزاری برای دور زدن فیلترینگ است که از فناوری‌های وی‌پی‌ان، اس‌اس‌اچ و اچ‌تی‌تی‌پی استفاده می‌کند تا دسترسی بدون سانسور به محتوای اینترنت را برای شما فراهم کند. این اپلیکیشن به صورت خودکار به نقاط دسترسی جدید پی می‌برد تا احتمال دور زدن فیلترها را برای شما بالا ببرد.

سهولت استفاده

کار کردن با «سایفون» خیلی راحت است. فقط لازم است آن را از طریق یکی از لینک‌های بالا روی دستگاه خود دانلود و نصب کنید. بعد از اینکه نصب شد، اپلیکیشن را باز کنید و روی 'connect' بزنید تا «سایفون» روی دستگاه فعال شود..

مزایا و ویژگی‌ها

«سایفون» سابقه‌ی طولانی در دور زدن سانسور اینترنتی در ایران دارد و همچنان برای این منظور کارایی خود را حفظ کرده است.

هر چند در زمان‌های وقوع اختلال در اینترنت و یا قطع کامل از کارایی آن کم می‌شود، بخش کوچکی از کاربران «سایفون» گزارش داده‌اند که طی قطع شدن اینترنت در آبان ۱۳۹۸ به محتوای اینترنت جهانی دسترسی داشته‌اند. تحقیقات مکملی که از سوی«سایفون» صورت گرفت نیز صحت این موضوع را تایید کرد.

در نسخه‌ی ۵.۰ و بالاتر اندروید فیلترشکن سایفون، امکان غیر فعال کردن برنامه‌هایی که نمی‌خواهید از تونل سایفون رد شوند را دارید.

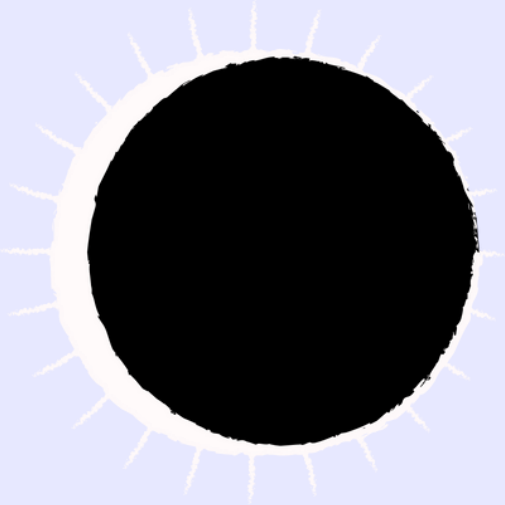
بدین ترتیب می‌توانید از این فیلتر شکن هدفمندتر استفاده کرده و در مصرف حجم اینترنت نیز صرفه جویی کنید.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

باگر دنبال دست یافتن به اطلاعات حساس یا به اشتراک گذاشتن آن هستید، نباید فقط به این اپلیکیشن متکی باشید.

هرچند که با استفاده از «سایفون»، ISP شما قادر به دیدن محتوای در حال داد و ستد شما نخواهد بود، اما این اپلیکیشن مانع این نمی‌شود که تاریخچه مرورگر و کوکی‌ها بر روی دستگاه شما ذخیره نشوند.

توجه داشته باشید که «سایفون» برخی اطلاعات در رابطه با ناحیه، کشور و فعالیت‌های انجام شده روی مرورگر شما و زمان و تاریخ آن ها را ثبت می‌کند. برنامه‌نویسان «سایفون» این داده‌ها را جمع‌آوری و تحلیل کرده و سپس آن‌ها را حذف می‌کنند. خط مشی «سایفون» در رابطه با حفظ حریم خصوصی به زبان فارسی در اینجا موجود است، که در مورد جمع‌آوری داده‌ها و نحوه‌ی به اشتراک گذاشتن آن‌ها با طرف ثالث در آن توضیح داده شده است.



جعبه ابزار خاموشی کامل

قطع اینترنت در آبان‌ماه ۱۳۹۸ یک فاجعه بود.
اما برای اتفاقات مشابهی که در آینده ممکن است پیش بیاید، با برقراری شبکه ملی اطلاعات ممکن است گزینه‌های محدودی برای برقراری ارتباط باقی بگذارد و شانس‌های اندکی برای ابزارهای دور زدن ایجاد کند تا بتوان به اینترنت جهانی دست پیدا کرد.
اما در صورتی که همه چیز کاملاً قطع شود چه گزینه‌های خواهیم داشت؟
انتخاب‌ها محدود هستند، اما چند گزینه وجود دارد. جعبه‌ابزار خاموشی کامل، مروری است بر چند ابزاری که می‌توانند از قطع ارتباط کامل شما در زمانی که هم اینترنت جهانی و هم اینترنت ملی خاموش شده باشند، جلوگیری کنند.

دریافت یک‌طرفه‌ی محتوا از طریق ماهواره – رابطی بسیار مهم به دنیای بیرون

توصیه‌ی ما در اینجا مشابه توصیه‌ای است که در بخش جعبه‌ابزار قطع اینترنت برای شما داشتیم: سرویس پخش ماهواره‌ای «توشه» به احتمال زیاد بهترین فرصت را برای دسترسی به اطلاعات فیلتر نشده و مرتب به‌روزرسانی شده از دنیای بیرون، فراهم می‌کند تا از اخبار مطلع شوید و در زمان بحران امنیت خود را حفظ کنید.
در صورت خاموشی کامل، «توشه» علاوه بر بسته‌های محتوای معمول خود، محتوای افزوده‌ای منتشر خواهد کرد، این محتوا شامل به‌روزرسانی درباره وضعیت اینترنت خواهد بود، و همچنین هرگونه توصیه‌ای درباره اینکه چطور می‌توانید در زمان بحران به شکلی امن به اطلاعات دسترسی پیدا کنید و با دیگران ارتباط برقرار کنید.
اگر نگران وقوع یک خاموشی کامل هستید، باید به صورت جدی نصب توشه را در اولویت قرار دهید، چون زمانی که خاموشی اتفاق بیفتد دیگر دیر خواهد بود.

Tooshe

Android | Windows | Linux

فناوری مورد استفاده در توشه این امکان را فراهم می‌کند که داده‌های غیر ویدیویی را به پخش زنده‌ی تلویزیونی تبدیل کند. داده‌ها دسته‌بندی می‌شوند، روی یک سرور بارگذاری می‌شوند، توسط ماهواره‌های موجود پخش می‌شوند و بعد توسط کاربران ضبط و رمزگشایی می‌شوند. این کار به کاربران این اجازه را می‌دهد تا در صورت قطع موقت و یا کامل اینترنت، به اخبار، اطلاعات و منابعی که از خارج از کشور فرستاده می‌شود دسترسی پیدا کنند

سهولت استفاده

یک «یو-اس-بی فلش درایو» ساده که به دستگاه رسیور (گیرنده دیجیتال) وصل شده است، اطلاعات را ذخیره می‌کند، سپس کاربر فلش درایو را به یک تلفن همراه یا کامپیوتر وصل می‌کند و توسط نرم‌افزار رمزگشایی و مشاهده‌ی فایل «توشه» محتوا را به شکل اولیه‌ی آن مشاهده می‌کند.

اپلیکیشن توشه از مرداد ماه ۱۴۰۱ بر روی سیستم عامل لینوکس نیز قابل استفاده است.

راهنمای نصب و استفاده این اپلیکیشن رمزگشایی و مشاهده فایل را می‌توانید روی وب سایت «توشه» که در بالا لینک شده است پیدا کنید.

همچنین داده‌های توشه را می‌توانید از طریق: ماهواره: یاه سَت | فرکانس: ۱۱۷۶۶| سیمبل ریت: ۲۷۵۰۰ | پولاریزاسیون: عمودی، دریافت کنید.

مزایا و ویژگی‌ها

هر وقت در ایران یک اختلال اینترنتی بوجود می‌آید، «توشه» یک بسته‌ی روزانه به اشتراک می‌گذارد که شامل ابزارهای «پروکسی»، اپلیکیشن‌های پیام‌رسان رایج (به همراه بروزرسانی) ، آموزش امنیت دیجیتال، اپلیکیشن‌های اشتراک گذاری فایل، ابزارهای حریم خصوصی و بسته‌های مخصوص تظاهرات، می‌باشد.

فناوری پخش ماهواره‌ای داده‌ی «توشه» قادر است تا اطلاعات را در قالب‌های مختلف، و نه فقط ویدیو، پخش کند. پی‌دی‌اف، جی‌پگ، اچ‌تی‌ام‌ال، ام‌پی‌تری یا هر قالب دیگری که باشد، هنگامی که کاربر شبکه‌ی ماهواره‌ای را ضبط می‌کند، جمع‌آوری می‌شود.

فناوری «توشه» به وسیله برقراری ارتباط یک‌طرفه، به شکلی امن و بدون فاش شدن هویت افراد عمل می‌کند. از آنجایی که اطلاعات به همان شکل تلویزیون ماهواره‌ای به اشتراک گذاشته و دریافت می‌شود، محتوای مورد نظر کاربران قابل نظارت نخواهد بود و اطلاعات شخصی افراد هیچگاه جمع‌آوری و یا به اشتراک گذاشته نمی‌شود.

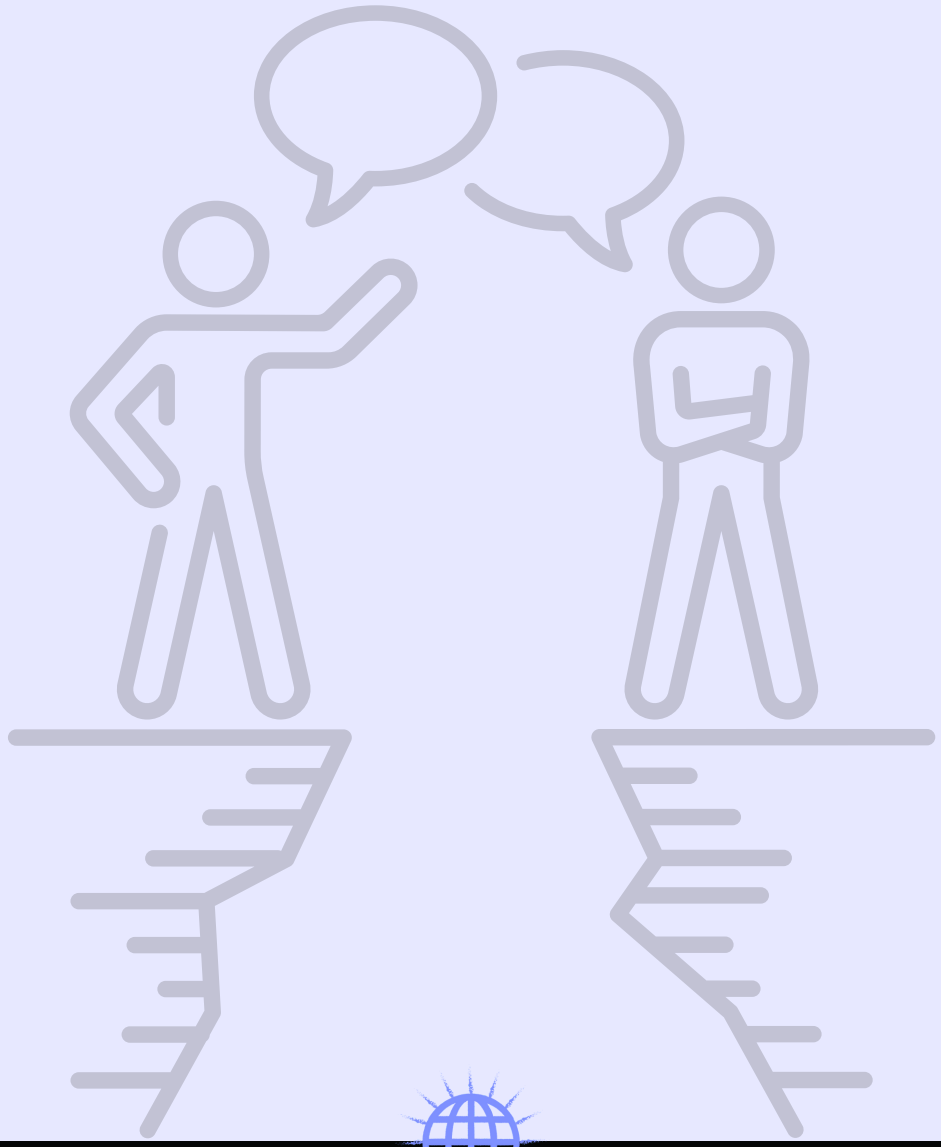
خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

از «توشه» نمی‌توانید بنا به میل خود برای گشت‌زنی در اینترنت استفاده کنید، فقط این امکان را دارید تا محتوایی که توشه جمع‌آوری و پخش می‌کند را دانلود کنید.

از آنجایی که پخش اطلاعات به صورت یکطرفه انجام می‌شود، نمی‌توانید از توشه برای برقراری ارتباط با افراد دیگر و یا فرستادن فایل به خارج از کشور، استفاده کنید. کاربرد توشه عمدتاً ایجاد دسترسی به اطلاعات حیاتی در مواقع بحرانی می‌باشد.

اپلیکیشن‌های پیام‌رسان - برقراری ارتباط در زمان خاموشی

اگر شبکه ملی اطلاعات از کار بیفتد، دیگر هرگونه گزینه‌ی آزمایشی مانند «جمی» که برقراری ارتباط را از طریق شبکه ملی اطلاعات فراهم می‌کند، امکان‌پذیر نخواهد بود.
در چنین شرایطی، بهترین گزینه می‌تواند بهره‌برداری از شبکه‌های محلی وای‌فای برای کار با «برایر» باشد - البته برای این منظور شما و فردی که می‌خواهید با او ارتباط برقرار کنید، هر دو باید بر روی یک شبکه‌ی مشترک قرار داشته باشید. این روش می‌تواند برای رد و بدل کردن فایل‌های صوتی و تصویری بین دو دستگاه به کار بیاید، اما به احتمال زیاد اگر این فرد در این حد به شما نزدیک است، پس می‌توانید او را رو در رو ببینید.
این ابزار، برقراری ارتباط از طریق بلوتوث را نیز فراهم می‌کند. با این حال خطرات و نقص‌های امنیتی در برقراری ارتباط بلوتوثی وجود دارد، این ابزار در زمانی که شما بین جمعیت هستید و واقعا نیاز دارید با دوستانتان در نزدیکی خود در ارتباط بمانید، می‌تواند به کار شما بیاید. بلوتوث خود را فعال نکنید مگر وقتی که مطمئن باشید به ریسکش می‌ارزد.



Briar

Android | F-Droid app

««برایر» یک اپلیکیشن پیام‌رسان است که برای استفاده کنشگران، روزنامه‌نگاران و هر کس دیگری که احتیاج به برقراری ارتباط در زمان قطع اینترنت داشته باشد، طراحی شده است. برخلاف اپلیکیشن‌های پیام‌رسان سنتی، «برایر» متکی بر یک سرور مرکزی نیست، پیام‌ها با استفاده از یک شبکه توری به صورت مستقیم بین دستگاه‌های کاربران همزمان‌سازی یا همان synchronized می‌شوند.

سهولت استفاده

کاربران می‌توانند «برایر» را برای اندروید از پلی استور گوگل، F-Droid یا وب سایت برایر دانلود نمایند..

مزایا و ویژگی‌ها

«برایر» می‌تواند برای به اشتراک گذاشتن پیام‌های مهم با افرادی که به آن‌ها اعتماد دارید، به شکلی مطمئن عمل کند. در هنگام قطع شدن اینترنت، این اپلیکیشن اجازه می‌دهد تا داده‌ها و اطلاعات را با لیست مخاطبان(کانتکت‌ها) خود به شکلی امن به اشتراک بگذارید، البته لازم خواهید داشت تا با فرد گیرنده در محدوده‌ی بلوتوث یا روی یک شبکه وای‌فای مشترک قرار داشته باشید.

علاوه بر قابلیت گپ زدن سرتاسری خصوصی و گروهی، «برایر» به شما این امکان را می‌دهد تا تالارهای گفتگوی عمومی و بلاگ‌هایی تشکیل دهید که برقراری ارتباط را با گروه‌های معتمد میسر می‌سازد، و حتی در زمان‌های قطع اینترنت هم قابل اشتراک‌گذاری و به‌روزرسانی هستند.

تالارهای گفتگو، مکالمات غیر خصوصی هستند. بر خلاف گروه‌های خصوصی، هر کسی که به آن بپیوندد می‌تواند کانتکت‌های دیگر خود را به تالار دعوت کند. در ضمن بلاگ‌ها امکان پست و به اشتراک گذاشتن اخبار و بروزرسانی‌ها را با تمام کانتکت‌هایتان امکان پذیر می‌سازند.

«برایر» همچنین با اپلیکیشن "دکمه هشدار" Ripple مجهز شده است که می‌تواند برایر را مخفی کند یا در حالتی که نگران هستید حساب کاربری شما تحت نظارت قرار گرفته یا مصادره شده، می‌تواند طوری پیکربندی شود که حساب کاربری و تاریخچه پیغام‌های شما را پاک کند.

خطرات و آنچه این اپلیکیشن انجام نمی‌دهد

این اپلیکیشن البته اشکالاتی نیز دارد. گزارش‌هایی از مشکلات برقراری ارتباط از طریق بلوتوث در زمانی که اینترنت قطع شده است دریافت شده، اما گروه «برایر» مشغول رفع این اشکالات هستند.

در زمان قطع اینترنت، این اپلیکیشن تنها در صورتی که کاربران در محدوده بلوتوث و وای‌فای یکدیگر قرار داشته باشند، می‌تواند کارایی داشته باشد.

مشکل دیگر این اپلیکیشن این است که تا زمانی که تعداد زیادی از افراد شروع به استفاده از «برایر» نکنند، نمی‌تواند در زمان‌های قطع دسترسی به اینترنت از تمام امکانات بالقوه خود استفاده کند و موثر واقع شود. برای اینکه «برایر» بتواند به یک اپلیکیشن پیام‌رسان قدرتمند تبدیل شود و جایگزین پیام‌رسان‌های معمول بشود، می‌بایست تعداد کاربران گسترده‌ای را جذب کند.

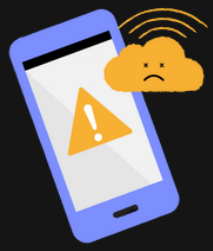
ابزارهای دور زدن – یک بن‌بست

اگر شبکه ملی اطلاعات به شکل کامل قطع شود، بسیار بعید است که ابزارهای دور زدن مانند «سایفون» بتوانند راهی به اینترنت جهانی پیدا کنند. بنابراین به‌هیچ‌وجه نباید از این اپلیکیشن‌ها انتظار داشته باشید که در صورت خاموشی کامل عمل کنند.
در عوض، پیشنهاد می‌کنیم که از «توشه» (که در بالا توضیح دادیم) به عنوان آخرین راه‌حل استفاده کنید تا در زمان خاموشی کامل، به اطلاعات بیرون از کشور دسترسی بیابید.

filterbaan

filter.watch

با به اشتراک گذاشتن عملکرد این ابزارها در زمانه خاموشی و قطعی اینترنت، به ما برای اطلاع‌رسانی در این زمینه و کمک به ایجاد دسترسی برای دیگر کاربران در ایران یاری رسانید



کانال تلگرام ما: Filter_Watch

www.Irandarkhamooshi.net

ایران در خاموشی