ایران در خاموشی

@FILTERBAAN

جعبه ابزار همراه

ابزار و توصیه‌های کاربردی برای حفاظت از امنیت دیجیتال هنگام شرکت در اعتراضات

برای دانلود ابزار معرفی شده در این پست به وبسایت ما مراجعه کنید

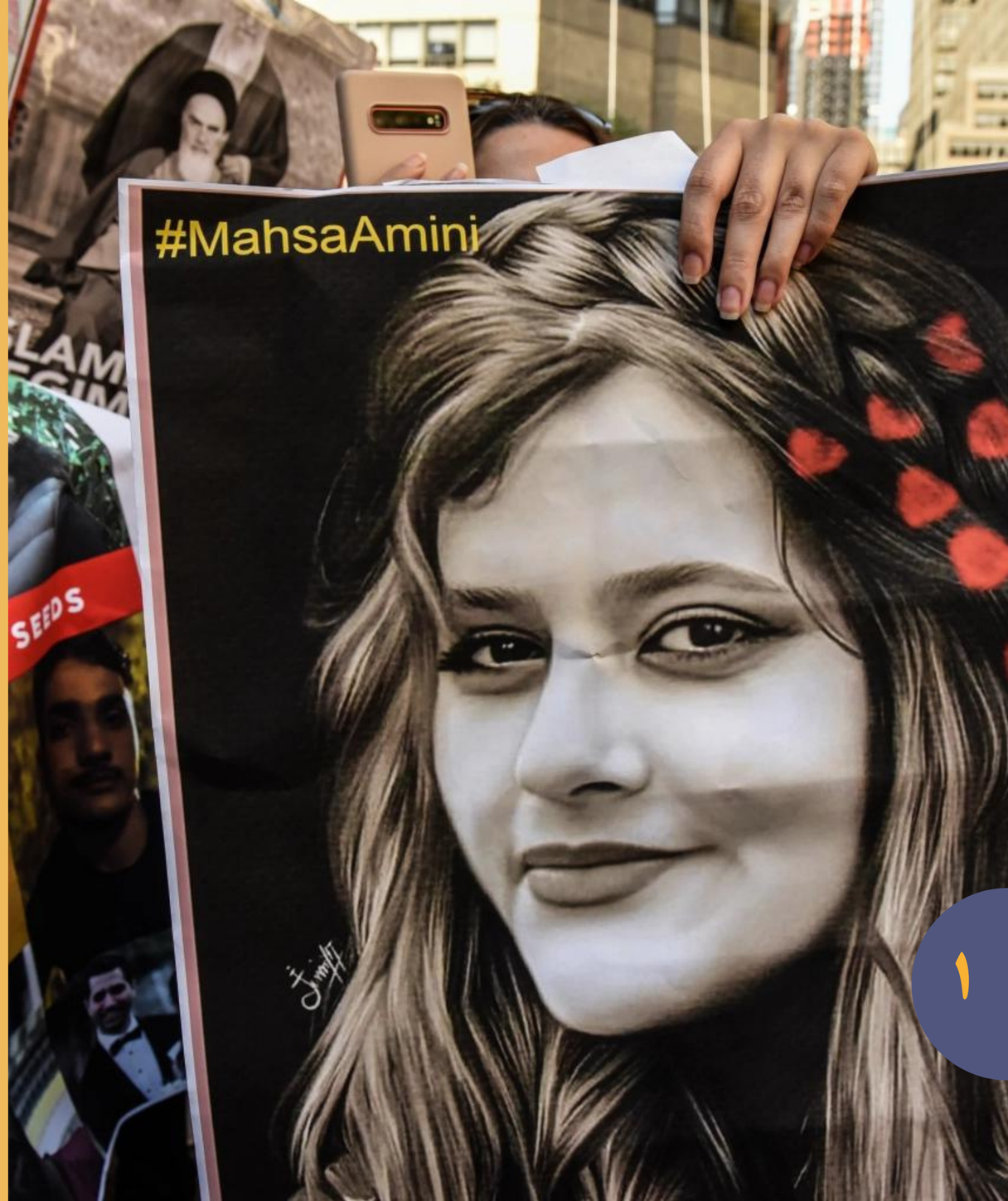
WWW.IRANDARKHAMOOSHI.NET

FILTER WATCH

مقدمه

با گسترش استفاده از گوشی‌های هوشمند در ایران، متهم کردن مخالفان، معترضان و دگراندیشان براساس مستندات به دست آمده از تلفن همراه به روندی معمول برای نیروهای امنیتی بدل شده است.
از شروع اعتراضات سراسری به مرگ مهسا امینی و فراگیر شدن جنبش برآمده از آن «زن، زندگی، آزادی» و به تبع آن بازداشت و سرکوب گسترده‌ی معترضان توسط حکومت ایران، این موضوع مجددا مورد توجه قرار گرفته است.
هرچند گزارش‌های غیررسمی بسیاری از اتهامات مبتنی بر مستندات به دست آمده از تلفن همراه حکایت دارد، کمیته پیگیری وضعیت زندانیان در گزارش سوم خود اعلام کرده که دست‌کم یک نفر براساس فیلم‌هایی که از گوشی موبایل او استخراج شده و همچنین محتویات اینستاگرامش به محاربه متهم و به اعدام محکوم شده است.

ما در «ایران در خاموشی»، در مجموعه‌ی پیش رو، تعدادی از اپلیکیشن‌های کاربردی را گردآوری کردیم تا به بالا بردن امنیت دیجیتال شما برای شرکت در تظاهرات یا برنامه‌های اعتراضی کمک کند. جز این، توصیه‌هایی جمع‌آوری کرده‌ایم تا احتمال دسترسی دیگران به داده‌های شخصی و اکانت‌های شبکه‌های اجتماعی‌تان را تا حد ممکن پایین بیاورید.
ضرورت رعایت این نکات از آن روست که می‌توان گفت، تقریبا تمام داده‌های موجود در تلفن همراه نظیر ویدیو، عکس، نوشته، تاریخچه‌ی مرورگر و سایت‌های بازدیدشده، تاریخچه‌ی موتور جستجو، گفتگوهای ذخیره شده در برنامه‌های پیام‌رسان، ایمیل‌های تبادل شده، موقعیت مکانی و اطلاعاتی از این دست می‌توانند برای پرونده‌سازی علیه شرکت‌کنندگان در اعتراضات و فعالین سیاسی و مدنی، مورد استفاده قرار بگیرند.
توصیه‌ها و ابزارهای این مجموعه در سه بخش کلی ارائه شدند. بخش اول ارتباط امن و آمادگی پیش از حضور در تجمع‌ها، بخش دوم ابزارها و توصیه‌هایی برای شرکت در تظاهرات و بخش سوم اقداماتی در صورت دستگیری احتمالی یا ضبط تلفن همراه.
شما می‌توانید با به اشتراک گذاشتن این توصیه‌ها با دوستان و اطرافیانتان به امنیت دیجیتال آن‌ها کمک کنید.



درباره‌ی ما

وبسایت «ایران در خاموشی» پس از قطعی اینترنت در آبان ۹۸ شکل گرفت تا بتواند امکان دسترسی کاربران به دنیای آزاد را – در صورت اختلال اینترنت یا برقراری اینترانت ملی – فراهم کند. به همین منظور، ابزارهای کاربردی که می‌توانند این دسترسی را برقرار کنند، در این سایت گردآوری شده‌اند.

فعالیت اصلی ما در ایران در خاموشی، فراهم آوردن چهار جعبه ابزار برای رویارویی با چهار وضعیت مختلف اینترنت است. جعبه ابزار روزمره، جعبه ابزار اختلال در اینترنت، جعبه ابزار قطع اینترنت و جعبه ابزار خاموشی کامل. در این چهار مجموعه، ابزارهایی برای برقراری ارتباط، گشت و گذار امن در فضای مجازی، دور زدن فیلترینگ و کسب اطلاعات در هنگام خاموشی اینترنت فراهم شده است.

همه‌ی این ابزارها توسط کارشناسان امینت دیجیتال ما بررسی و بر پایه‌ی سه شرط اساسی «کارایی»، «امنیت» و «قابل استفاده برای عموم بودن» دست چین شده‌اند. این جعبه ابزارها همچنین به زبان‌های ترکی، کردی و بلوچی ترجمه شده‌اند که به زودی منتشر می‌شوند .

امید ما این است که با جستجو و یافتن ابزارهای مختلف، بررسی و امینت سنجی، و ارائه‌ی آن‌ها به زبان و اشکالی ساده، در ایجاد دسترسی شما به دنیای آزاد اطلاعات کمک کنیم چرا که معتقدیم اختلال و قطع اینترنت به شکلی بنیادین حقوق بشر را هم در فضای آنلاین و هم در دنیای واقعی نقض می‌کند.

ایران در خاموشی پروژه‌ای است که سازمان میان‌گروه آن را اداره می‌کند. این وب‌سایت برای نخستین بار توسط سازمان ***Small Media*** راه‌اندازی شده بود.

بخش اول: ارتباط امن و آمادگی پیش از حضور در تجمعات

این بخش که شامل اصول پایه‌ای امنیت دیجیتال است، برای فعالیت‌های مجازی روزمره مفید و برای آمادگی پیش از حضور در تجمعات ضروری است.
این توصیه‌ها شامل برقراری ارتباط از طریق پیام رسان‌های امن، رمزگذاری پیام‌ها و تصاویر ارسالی، پاک سازی و خروج از حساب‌های کاربری شبکه‌های اجتماعی، پاک‌سازی داده‌های مهم از روی گوشی و استفاده از رمزهای دو مرحله‌ای و پیچیده برای جلوگیری از بازگشایی حساب‌های کاربری شما توسط نیروهای امنیتی است.
اینها نکات ساده‌ای هستند که سهل‌انگاری در رعایت کردن آن‌ها می‌تواند نه تنها امنیت شما بلکه دوستان و همراهانتان را به خطر بیندازد.

استفاده از پیام‌رسان امن

برای برنامه‌ریزی و هماهنگی با دیگران از پیام‌رسان‌های امن یا برنامه‌هایی که امکان رمزگذاری پیام را فراهم می‌کنند، استفاده کنید. بارها شاهد بوده‌ایم که با استخراج محتوای رد و بدل شده در پیام‌رسان‌های یک شخص، تنها به خاطر یک قرار ساده در محل اعتراضات، او را به جرم اجتماع و تبانی یا حتی جلوداری (لیدری) اعتراضات متهم کرده‌اند.
پیامک تلفنی و پیام‌رسان‌های بومی هرگز راه‌های ارتباطی امنی نیستند. بنابراین تحت هیچ شرایطی از پیام‌رسان‌های داخلی استفاده نکنید.

استفاده از پیام‌رسان امن

در مورد دو پیام‌رسان رایج واتساپ و تلگرام نیز بهتر است در به اشتراک گذاشتن موارد امنیتی و مهم، جانب احتیاط را رعایت کنید.
تلگرام به صورت پیش‌فرض پیام‌های شما را رمزنگاری نمی‌کند و برای این کار حتما باید گزینه‌ی سکرت چت (چت امن) را انتخاب کنید. پاک کردن خودکار پیام‌ها نیز تنها در صورت استفاده از این گزینه فراهم است. همچنین این برنامه فراداده‌های (متا دیتا) زیادی را حداقل تا دوازده ماه در برنامه حفظ می‌کند.

هرچند واتس‌اپ به صورت پیش‌فرض پیام‌های شما را رمزگذاری و از پروتکل‌های امنی پیروی می‌کند اما همواره میزان داده‌ای که این برنامه با شرکت اصلی خود «متا» و به واسطه‌ی آن دلالان داده به اشتراک می‌گذارد، نگرانی‌هایی وجود دارد. همچنین گزارش‌های غیررسمی وجود دارد که ممکن است برخی از پیام‌ها حتی بعد از پاک شدن در این اپلیکیشن قابل بازیابی باشند.

از نگاه کارشناسان ما، پیام‌رسان‌های زیر امن‌ترین امکان تبادل اطلاعات را فراهم می‌کنند:

پیام‌رسان سیگنال

این پیام‌رسان برای ویندوز، اندروید و آی‌اواس قابل استفاده است و پیام‌ها در هر دو طرف مکالمه رمزگذاری می‌شوند. به عبارت ساده‌تر، اگر خط شما شنود شود، نهاد شنود کننده - در پیشرفته‌ترین حالت- به یک سری اطلاعات رمز شده دسترسی دارد و عملا نمی‌تواند پیام را بخواند. اگر امکان حذف خودکار پیام‌ها را فعال کرده باشید، پیام‌تان مدتی پس از ارسال به مخاطب، پاک شده و در دسترس کسی نخواهد بود. این پیام رسان البته تنها از طریق اینترنت قابل استفاده است و بدون آن کارایی ندارد.

پیام‌رسان سشن

این پیام‌رسان امکان نصب روی ویندوز،ا ندروید و ای‌آواس را دارد. تفاوت این پیام‌رسان با سیگنال این است که، برای راه‌اندازی به شماره تلفن کاربر نیازی ندارد. در نتیجه، بلاک یا شنود شدن پیامک فعال‌سازی تاثیری روی دسترسی شما به این سامانه ندارد. هیچ داده و ابرداده (متا دیتا) در این برنامه نگهداری نمی‌شود. در نتیجه، حتی اگر تلفنتان به دست نهادهای امنیتی افتاده و رمز ان را هم داشته باشند، عملا نمی‌توانند به اطلاعات خاصی دسترسی پیدا کنند.
به خصوص اگر امکان حذف خودکار پیام‌ها را فعال کرده باشید، پیام‌تان مدتی پس از ارسال به مخاطب، پاک شده و در دسترس کسی نخواهد بود.

ابزار رمزگاری نهفت

نهفت پیام رسان نیست اما با کمک آن می‌توانید پیام‌هایتان را پیش از ارسال رمزگذاری کنید. این برنامه که توسط گروه «همبستگی برای ایران» تهیه شده، فعلا فقط روی سیستم عامل اندروید قابل پیاده‌سازی است. با کمک این سامانه می‌توانید پیام‌هایتان را پیش از فرستادن برای دیگران رمزگذاری کنید تا محتوای آن قابل شناسایی نباشد. برای راه‌اندازی این برنامهبه ارتباط اینترنتی یا شماره تلفن نیازی ندارید. شما همچنین می‌توانید اطلاعات رمزگذاری شده را از طریق هر پیام‌رسانی، حتی بر روی شبکه ملی اطلاعات ارسال کنید. اطلاعاتی مربوط به شما یا تلفن همراه‌تان نیز روی سرورهای «نهفت» ذخیره نمی‌شود.

مهم

در تمام اپلیکیشن‌های پیام‌رسان حتما امکان حذف پیام خودکار را فعال کنید. با این تنظیمات، پیام‌های شما برای دیگران بعد از زمان مشخصی (مثلا یک ساعت بعد از خوانده شدن) پاک می‌شود.
ضمنا توجه داشته باشید که، پیام‌رسان‌هایی که از آنها نام بردیم زمانی کار می‌کنند که ارتباط اینترنتی برقرار باشد. بدون اینترنت این نرم‌افزارها کارایی ندارند. در ادامه همین مطلب به پیام‌رسان‌هایی نیز اشاره کرده‌ایم که در صورت قطع اینترنت احتمالا کار می‌کنند و می‌توانند ارتباط شما با اطرافیان را برقرار کنند.

حفاظت از داده‌ها، قبل از شرکت در تجمع

توصیه‌ی کارشناسان ما در این زمینه روشن است:

در هیچ برنامه اعتراضی تلفن‌تان را با خود نبرید.

اما اگر ناچار به همراه بردن تلفن خود هستید، به این نکته‌ها توجه کنید:

۱ حساب‌های کاربری‌تان را خصوصی/پرایوت کنید

تمام حساب‌های کاربری‌تان در تمام شبکه‌های اجتماعی را از حالت عمومی خارج کنید و به حالت پرایوت یا خصوصی در بیاورید. در این حالت، دیدن محتوایی که در حسابتان - مثلا در اینستاگرام - منتشر می‌کنید، برای عموم مردم و کسانی که در لیست دوستان شما نیستند، امکان‌پذیر نیست.
برای انجام این‌کار می‌توانید به بخش تنظیمات حساب کاربری‌تان بروید و گزینه «پرایوت» را انتخاب کنید. برای دسترسی به بخش «تنظیمات» باید روی آیکون چرخ‌دنده یا سه‌نقطه کلیک کنید. ممکن است عبارت «تنظیمات حساب کاربری» یا Setting در بعضی حساب‌های کاربری درج شده باشد.

۲ رمزهای قوی استفاده کنید

برای تلفن همراه‌تان رمزهای قوی (شامل اعداد و حروف بزرگ و کوچک و نشانه‌های مختلف) انتخاب کنید تا بازیابی آن برای نیروهای امنیتی و افرادی که ممکن است تلفن شما را تحت نظر بگیرند، دشوارتر باشد. همچنین این اصل را در مورد رمز شبکه‌های اجتماعی و ایمیلتان هم مراعات کنید. سال تولد، یک سری عدد پشت سر هم، نام خودتان یا اطرافیان‌تان و... رمزهای ضعیفی هستند. همچنین اگر تلفن همراه‌تان از قابلیت قفل تشخیص چهره یا اثر انگشت پشتیبانی می‌کند، حتما آن را فعال کنید.

۳ از تمام حساب‌های کاربری‌تان خارج شوید

از تمام حساب‌های کاربری‌تان اعم از ایمیل، شبکه‌های اجتماعی و پیام‌رسان‌ها- خارج شوید. به خصوص اگر احتمال دستگیری‌تان وجود دارد، حتما این‌کار را انجام دهید.

۴ اپلیکیشن‌های داخلی را حذف کنید

بهتر است تمام اپلیکیشن‌های داخلی را از گوشی‌تان حذف کنید. به دلیل دسترسی این اپلیکیشن‌ها به داده‌های گوشی ممکن است نیروهای امنیتی بتوانند به این اطلاعات دسترسی پیدا کرده و برایتان پرونده‌سازی کنند.

۵ رمز دو مرحله ای را از پیامک به ایمیل تغییر دهید

امکان ورود با رمز دو مرحله‌ای یا ۲FA را برای همه حساب‌های کاربری‌تان - ایمیل و شبکه‌های اجتماعی - فعال کنید. در این صورت، بعد از وارد کردن رمز عبور (پسورد) از شما یک کد یکبار مصرف درخواست خواهد شد.
امکان دریافت این رمز با پیامک را غیرفعال کنید چون نهادهای امنیتی امکان شنود و دسترسی به پیامک‌های ارسالی را دارند. در عوض، امکان دریافت کد ورود دومرحله‌ای با اپلیکیشن‌های Authenticator را فعال کنید. این برنامه‌ها، همان رمز دوم را برایتان نمایش خواهند داد.

۶ اطلاعات مهم را پاک کنید

اگر روی اکانت‌های شخصی شبکه‌های اجتماعی، ایمیل یا داخل تلفن همراه‌تان محتوای حساسیت‌برانگیز و مهمی دارید، آن را حذف کنید. محتوای خطرناک یعنی هرچیزی که بتواند امکان پرونده‌سازی برای شما را فراهم کند یا موقعیت و سلامت دوستان‌تان را به خطر بیندازد.
مراقب باشید که داده‌هایتان از همه‌جا پاک شده باشند. بعضی از عکس‌ها و داده‌ها به طور خودکار توسط تلفن همراه‌تان پشتیبان‌گیری شده و در جای دیگری - مثلا یک فضای ابری- ذخیره می‌شوند. اگر داده مهمی را دارید که نمی‌خواهید به دست کسی بیفتد، مطمئن باشید که نسخه‌های پشتیبان نیز پاک شده‌اند.

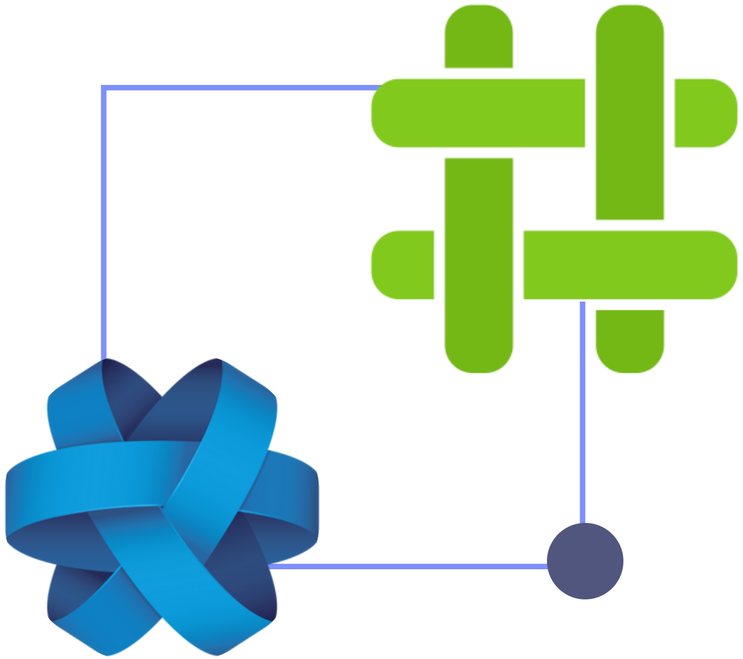
بخش دوم–ابزارها و توصیه‌هایی برای شرکت در اعتراضات

تکرار این نکته ضروری است که کارشناسان ما معتقند، همراه نبردن تلفن همراه بهترین گزینه برای شرکت در تجمعات و مکان‌هایی با خطر دستگیری است.
اما اگر ناچار به بردن گوشی خود شدید می‌توانید با رعایت چند نکته خطرات آن را کاهش دهید و یا برنامه‌هایی نصب کنید که ممکن است در موقعیت‌های پرخطر به کارتان بی‌آید.
این بخش شامل توصیه‌هایی برای جلوگیری از ردگیری شما چه به وسیله تلفن همراه و چه به وسیله تکنولوژی شناسایی چهره است. همچنین ما ابزارهایی را برای ایجاد ارتباط امن بدون اینترنت و در فواصل کوتاه معرفی میکنیم. دراین بخش ابزارهایی نیز برای فرستادن پیام اضطراری یا آخرین موقعیت مکانی شما قبل از بازداشت ارائه شده است.

حالت هواپیما را فعال کنید

پیش از رسیدن به مقصد گوشی را خاموش کنید یا روی حالت هواپیما قرار دهید. مطمئن شوید که همه دسترسی‌های داده – از جمله جی‌پی‌اس و آنتن موبایل، بلوتوث و ... – خاموش شده است.
برای این‌که بدانید از چه محلی به بعد باید تلفن همراه‌تان را خاموش کنید،به شیوه کارکرد و ردیابی آنتن‌های تلفن همراه دقت کنید. دکل‌های زمینی تلفن همراه موسوم به BTS به تلفن‌هایی که در محدوده ۵۰۰ مترمربعی‌شان در یک مساحت شش ضلعی قرار داشته‌باشند، خدمات ارایه می‌کنند. در نتیجه، حداکثر ۵۰۰ متر قبل از محل تجمع باید گوشی‌تان از دسترس خارج شده باشد.

همراه نبردن تلفن همراه بهترین گزینه برای شرکت در تجمعات و مکان‌هایی با خطر دستگیری است.



اپلیکیشن‌های مهم برای حضور در تجمع

اگر تلفن همراه‌تان را در اعتراضات همراه می‌برید، حتما این اپلیکیشن‌ها را نصب کنید. با این روش، می‌توانید با افراد دیگری که در تجمع حضور دارند، با یک راه امن در تماس باشید. ضمنا اگر توسط نیروهای امنیتی تهدید یا بازداشت شدید، می‌توانید این موضوع را به دیگران اطلاع دهید.

اپلیکیشن‌های Briar و Jami را نصب کنید

این برنامه‌ها به شما کمک می‌کنند که با اطرافیان‌تان ارتباط امن داشته باشید. با این برنامه‌ها می‌توانید به یک شبکه محلی امن - مثلا یک شبکه وای‌فای بدون اینترنت- متصل شوید و در یک فاصله حداکثر شش متری با یکدیگر در ارتباط بمانید.
توجه داشته باشید، برای این‌که بتوانید با دیگر اطرافیان و دوستان‌تان در تماس بمانید، باید آنها هم این نرم‌افزارها را نصب کنند. پس حتما به صورت گروهی این برنامه‌ها را نصب و استفاده کنید.

جمی یک برنامه پیام‌رسانی و تماس ویدیویی رمزگذاری‌شده است که به کاربران امکان می‌دهد پیام ارسال کنند، تماس برقرار کنند، تماس ویدیویی با یک یا چند نفر داشته باشند و کارهایی مانند اشتراک‌گذاری صفحه نمایش و اشتراک‌گذاری فایل‌ها مانند تصاویر را انجام دهند.

برایر به کاربران خود امکان می‌دهد تا بدون اینترنت و با استفاده از شبکه‌ای که توسط بلوتوث یا وای‌فای ایجاد می‌شود، با هم در ارتباط باشند. این به شما امکان می‌دهد تا در مواقع قطع یا اختلال در اینترنت بتوانید از این برنامه استفاده کنید. به دلیل این که شبکه‌های مانند بلوتوث و وای‌فای فقط توانایی ارتباط در فاصله مشخصی که چندان زیاد نیست را دارند، کاربران این اپلیکیشن باید در نزدیکی هم قرار داشته باشند. بلافاصله بعد از اتصال به اینترنت، امکان به اشتراک گذاشتن این اطلاعات با مخاطبینی که نزدیک شما نیستند نیز فراهم می‌شود.

از آنجایی که استفاده از این دو برنامه به ارتباط اینترنتی نیاز ندارد، در صورت قطع اینترنت یا از بین رفتن آنتن موبایل می‌توانید همچنان از آن استفاده کنید.

زمان شرکت در اعتراضات: مراقب سیستم‌های شناسایی چهره دیجیتال باشید

سیستم‌های شناسایی چهره می‌توانند از روی چهره شما به هویت‌تان پی ببرند. این سامانه چهره اشخاص را آنالیز کرده و محتوای آن را با یک بانک اطلاعاتی – مثلا داده‌های مربوط به کارت ملی هوشمند– می‌سنجد و آنها را شناسایی می‌کند. چنین سامانه‌هایی در حال حاضر در چین استفاده می‌شود و با کمک آن تا به حال فعالان مدنی بسیاری تحت فشار قرار گرفته‌اند. درباره چگونگی کارکرد سیستم مشابه در ایران، اطلاعات اندکی وجود دارد اما در عین حال شواهدی وجود دارد که از این سیستم در ایران استفاده می‌شود. در نتیجه بهتر است، نکات ایمنی در این باره را رعایت کنید:

از پوشیدن هر لباس یا در معرض دید قرار دادن هر چیزی که شما را قابل‌شناسایی کند مثل لباس‌های مارک‌دار، رنگی، طرح‌دار، مدل موی خاص و... اجتناب کنید.

چهره‌تان را با ماسک بپوشانید. به جز تشخیص چهره، ماسک می‌تواند در زمان شلیک اشک‌آور نیز به شما کمک کند.

اپلیکیشن Panic Button را نصب کنید

این برنامه به شما کمک می‌کند که در لحظه دستگیری – یا موارد مشابه– اطرافیان‌تان را از محل جغرافیایی‌تان در آن لحظه مطلع کرده و آنها را از شرایط‌تان باخبر کنید. این برنامه یک پیامک حاوی موقعیت جغرافیایی لحظه‌ای شما را به شماره تلفن‌هایی که از پیش تعیین کرده‌اید، پیامک می‌کند. شخص گیرنده برای دریافت پیام شما نیازی به نصب برنامه ندارد. این برنامه فعلا برای سیستم عامل اندروید در دسترس است.

نسخه‌ی مشابه و قابل استفاده برای کاربرانی که از گوشی‌های اپل استفاده می‌کنند برنامه‌ی Silent beacon است.

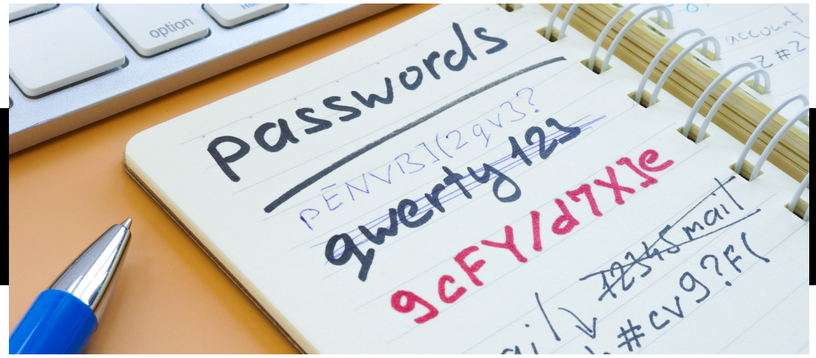
موقعیت جغرافیایی‌تان را با نزدیکان‌تان به اشتراک بگذارید

با استفاده از سرویس «نقشه گوگل» می‌توانید موقعیت جغرافیایی‌تان را با نزدیکان‌تان به اشتراک بگذارید. در نظر داشته باشید که، ممکن است سرویس‌های گوگل در ایران فیلتر شوند. در این صورت، انجام این کار منوط به باز ماندن فیلترشکن شماست. ضمن این‌که، استفاده از سرویس‌های نقشه روی موبایل، باتری زیادی مصرف می‌کنند.

بخش سوم– اقداماتی برای دستگیری احتمالی و یا ضبط تلفن همراه

بخش سوم- اقداماتی برای دستگیری احتمالی و یا ضبط تلفن همراه اگر توسط نیروهای امنیتی دستگیر شدید و تلفن‌تان در دست بازجوها ماند، می‌توانید به چند توصیه عمل کنید. توجه داشته باشید که برای انجام بخشی از کارهایی که در اینجا پیشنهاد می‌شوند، به افراد معتمد یا نزدیک نیاز خواهید داشت و خودتان احتمالا نمی‌توانید آنها را به تنهایی انجام دهید. به همین دلیل، پیشنهاد می‌کنیم، حتما این بخش از توصیه‌های ما را با یکی از افراد معتمد خودتان مرور کنید.

در این بخش همچنین توصیه‌هایی برای ارائه‌ی امن محتوای تهیه شده در اعتراضات اعم از عکس و ویدئو وجود دارد.



عوض کردن رمزهای عبور

اگر تلفن همراه‌تان دست نیروهای امنیتی باقی ماند، خودتان یا نزدیکان‌تان باید بتوانند رمز عبورتان را تغییر بدهید . این کار در صورتی امکان‌پذیر است که آنها راه دسترسی به حساب کاربری شما را بلد باشند.اگر شخص قابل اعتمادی در دسترس دارید می‌توانید ایمیلی که بر اساس آن حساب کاربری در شبکه‌های اجتماعی ساخته‌اید را در اختیار او قرار دهید تا در صورت ضرورت، به بازیابی حساب شما و کنترل و پاک سازی محتوای درون حساب اقدام کند.
تغییر رمز عبور با رفتن به بخش «تنظیمات حساب کاربری» یا «تنظیمات امنیتی» امکان‌پذیر است. (بنا به نوع شبکه اجتماعی یا ایمیل نام این بخش می‌تواند اندکی متفاوت باشد)

غیرفعال کردن امکان «دانلود اطلاعات» در فیسبوک

اگر عضو فیسبوک هستید، باید امکان دانلود اطلاعات را غیرفعال کنید. این‌کار با حذف یا غیرفعال کردن اکانت تفاوت دارد. در این‌حالت شما به کاربری که وارد حساب کاربری‌تان نمی‌شود اجازه نمی‌دهید که اطلاعات شخصی و محتوای فیسبوک شما را دانلود کند. برای انجام این‌کار از راهنمای فیسبوک استفاده کنید.

پاک کردن اطلاعات گوشی در اندروید

برای پاک کردن اطلاعات گوشی‌های اندروید باید به بخش تنظیمات یا Setting تلفن بروید. گزینه Allow Remote Lock and Factory Reset را انتخاب کنید. در پنجره جدیدی که باز می‌شود، گزینه «پیدا کردن دستگاه از راه دور» را انتخاب کنید. اکنون گزینه Allow remote lock and Factory reset را انتخاب کنید.

در مرحله بعد، یک صفحه جدید باز می‌شود که از شما اجازه می‌گیرد، داده‌های دستگاه‌تان را پاک کند. این صفحه را تایید کنید.

توجه داشته باشید، هنوز داده‌ای پاک نشده است. بلکه در اینجا شما به گوگل اجازه می‌دهید که، در آینده اگر نیاز شد، اطلاعات تلفن‌تان را از راه دور پاک کند.

برای پاک کردن داده‌های تلفن‌همراه اندرویدی باید به سایت «پیدا کردن» گوگل بروید. نام کاربری و کلمه عبورتان را وارد کنید. در این مرحله، موقعیت جغرافیایی تلفن شما را نشان می‌دهد. بعد از پیدا شدن تلفن، شما می‌توانید آن را قفل یا داده‌هایش را پاک کنید. اگر عبارت Erase را انتخاب کنید، داده‌ها – بعد اا‌ز تایید شما- از روی تلفن‌تان پاک می‌شوند. توجه داشته باشید که بعد از اعلام موافقت، از شما خواسته می‌شود تا یک‌بار رمزعبورتان را وارد کنید.

شما باید این تنظیمات را قبل از رفتن به تجمعات و مناطق پرخطر انجام دهید.

برای پاک کردن اطلاعات موبایل آیفون‌تان باید این مراحل را طی کنید:

با اپل‌آی‌دی و رمز عبور وارد حساب کاربری‌تان در سایت آی‌کلاود شوید. گزینه Find my phone را انتخاب کرده و از بین گزینه‌های موجود، Erase را انتخاب کنید. با تایید این مرحله تمام داده‌هایتان از روی گوشی پاک می‌شوند. اگر تلفن‌تان در آن لحظه به اینترنت وصل نباشد، در اولین زمانی که به اینترنت متصل شود، داده‌ها پاک می‌شوند.

یک راه دیگر هم برای محافظت از داده‌های شخصی‌تان در آیفون وجود دارد. در این‌صورت، حتی اگر تلفن‌تان به اینترنت متصل نشود، باز هم می‌توان امید داشت که اطلاعاتش پاک شود. در این حالت، وقتی شخص ثالث به گوشی شما دسترسی داشته باشد و ده بار پسورد اشتباه وارد کند، تمام اطلاعات داخل تلفن پاک می‌شود.

برای فعال کردن این امکان در آیفون باید وارد بخش تنظیمات یا Setting شوید و گزینه Face ID and Passcode را انتخاب کنید. در پنجره تازه گزینه Turne passcode را انتخاب کرده و یک پسورد جدید بسازید.

اگر قبلا پسورد ایجاد کرده‌اید، در همین صفحه گزینه Erase Date را فعال می‌کنید. در این‌صورت، همان‌طور که قبلا هم گفته شد، بعد از ده‌بار تلاش ناموفق در دسترسی به تلفن‌تان، تمام اطلاعات آن پاک می‌شود. برای این‌که چنین اتفاقی رخ بدهد، نیازی به اتصال اینترنتی نیست.

مهم

بعد از شرکت در اعتراضات؛ چطور اطلاع‌رسانی کنیم؟

تمام «متا دیتا» موجود روی عکس و ویدیوهایی که می‌خواهید در شبکه‌های اجتماعی به اشتراک بگذارید را پاک کنید. اینجا یک آموزش کوتاه وجود دارد. به عنوان یک راه‌حل برای حذف «ابر داده» یا «متا دیتا»، اگر از عکس‌هایتان اسکرین‌شات بگیرید، متادیتا حذف خواهد شد.

در پست‌هایی که در شبکه‌های اجتماعی منتشر می‌کنید، بخشی مربوط به چهره‌ها و لباس‌ها را محو کنید. برای انجام این‌کار در نرم‌افزارهای ویرایش ویدیو و عکس، یک فیلتر اختصاصی وجود دارد. (در منو دنبال گزینه‌ای به نام **Blur** بگردید.) وقتی عکسی را در پیام‌رسان سیگنال می‌فرستید، می‌توانید پیش از ارسال، محتوای آن را محو کنید. برای این‌کار عکس‌تان را انتخاب کنید. گزینه «ویرایش/**Edit** » را انتخاب کنید. گزینه **blur** **option** را انتخاب کنید. پیشنهاد ما این است که چهره‌ها، مارک لباس‌ها، نام خیابان‌ها و مکان‌های خاص و به طور کلی، هرچیزی که به شناسایی و دستگیری افراد کمک می‌کند را محو کنید.

ایران در خاموشی

سخن آخر

ما ویدیوهای کوتاهی از آموزش گام به گام ابزاری که در این مجموعه معرفی شده‌اند تهیه کرده‌ایم. برای بازدید این ویدیوها می‌توانید به صفحه‌ی ما در شبکه‌های اجتماعی مراجعه کنید

به یاد داشته باشید که با تمام دقت و کارشناسی که در مورد ابزار موجود در این مجموعه شده است، وجود باگ و حفره‌های امنیتی، بخشی از طبیعت ابزار دیجیتال و دنیای مجازی به حساب می‌آید. شما قبل از هر اقدامی در فضای مجازی باید بدانید که امنیت در این فضا صد درصدی نیست و همواره احتمالی را برای درز اطلاعات و رصد شدن در نظر بگیرید.

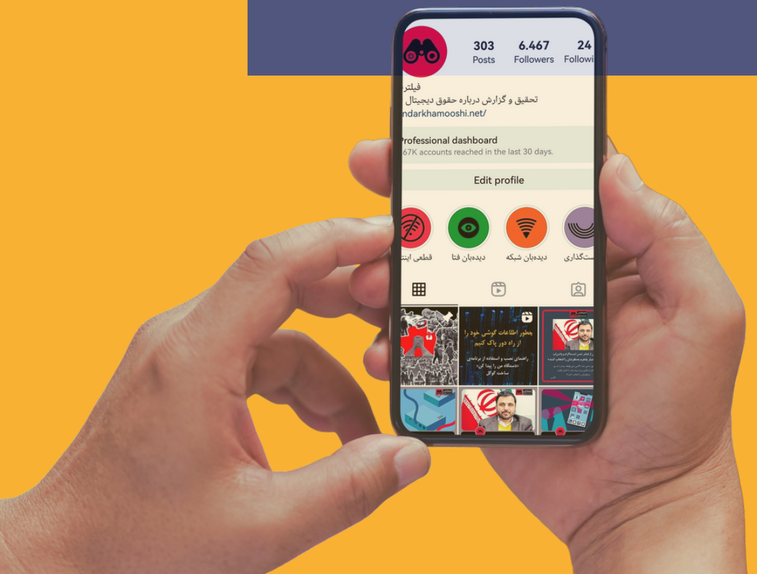
شما می‌توانید با در میان گذاشتن تجربیات شخصی، ملاحظات منطقه‌ای و به اشتراک گذاشتن دانش فنی خود در به روزرسانی و کاربردی‌تر کردن این جعبه ابزار همراه به ما کمک کنید.

راه‌های ارتباط با ما

@FILTERBAAN

@FILTER_WATCH

www.IRANDARKHAMOOSHI.NET



فیلترسان