****

آماده کردن گوشی‌های هوشمند برای مستندسازی آفلاین

به‌رغم خاموشی اینترنت، کسانی که قصد مستند کردن رویدادها را دارند، همچنان می‌توانند شواهد ویدئویی را ثبت و ضبط کنند و آن‌ها را یا به صورت آفلاین، یا بعد از بازیابی دسترسی به اینترنت، با دیگران به اشتراک بگذارند.

در این‌جا نکات و راهکارهایی را که از کنشگران و دیگر فعالان مستندسازی آموخته‌ایم، ارائه می‌کنیم تا بتوانید گوشی هوشمند خود را برای مستندسازی آفلاین آماده کنید.

توجه داشته باشید که برای برخی از مراحل این راهنما، دسترسی به اینترنت ضروری است. بنابراین باید این مراحل را یا پیش از وقوع خاموشی اینترنت انجام دهید یا پس از بازیابی دسترسی به اینترنت. برای انجام این مراحل، پیش از آن‌که در موقعیت پراسترس و پرخطر قرار بگیرید، اقدام کنید. همین حالا این گام‌ها را بردارید و با گوشی هوشمندتان تمرین کنید تا وقتی در شرایط بحرانی قرار می‌گیرید، کاملا آماده باشید.

قطعی اینترنت در اغلب موارد با تشدید محدودیت‌های اطلاعاتی و سرکوب آزادی بیان و تجمعات همراه می‌شود. اگر کارتان مستندسازی است، باید تمهیدات ویژه‌ای برای حراست از خودتان و اطلاعاتی که در این بازه‌های زمانی ثبت می‌کنید، بیاندیشید. اگر این خطر وجود دارد که ماموران گوشی هوشمندتان را مصادره کنند یا شما را وادار به بازکردن قفل آن کنند تا محتوای آن را بازرسی کنند (چه در شرایط خاموشی اینترنت یا هر شرایط دیگری) حتما از گوشی جداگانه‌ای برای مستندسازی استفاده کنید و گوشی اصلی‌تان را برای استفاده‌های شخصی نگه دارید. با این روش می‌توانید اطلاعاتی را که با خود حمل می‌کنید، به حداقل برسانید (که لیست دوستان، فهرست تماس‌ها، حساب‌های کاربری و پیام‌ها را در بر می‌گیرد). حتی اگر قادر به استفاده از گوشی جداگانه نیستید، همچنان می‌توانید از این راهنما برای کاستن میزان داده‌های حساس و ارتقای امنیت گوشی اصلی‌تان استفاده کنید.

اگر می‌خواهید از یک گوشی قدیمی‌تر استفاده کنید، اول اطلاعات موجود در آن را پاک‌سازی کنید

برای پاک‌سازی گوشی، با Factory Reset آن را به تنظیمات اولیه برگردانید.

نکته: مطالعات انجام‌شده نشان می‌دهند با Factory Reset همه داده‌های موجود روی گوشی‌ها حذف نمی‌شوند. در واقع، تنها راه صددرصد مطمئن برای پاک‌سازی همه اطلاعات موجود روی گوشی‌ها، نابود کردن گوشی است، اما بدیهی است که نابود کردن گوشی وقتی قصد استفاده مجدد از آن را دارید، جزو گزینه‌ها نیست. در مطلبی که در این لینک آمده، یکی از مهندسان اندروید پیشنهاد می‌کند که برای پاک‌سازی موثر، محتوای گوشی خود را پیش از Factory Reset رمزگذاری کنید. رمزگذاری، حالت پیش‌فرض روی اکثر گوشی‌های امروزی است، اما اگر نبود می‌توانید برای فعال کردن آن ابتدا به بخش تنظیمات (Settings) بروید، سپس در قسمت امنیت (Security) این گزینه (Encrypt Phone before resetting) را فعال کنید. به این ترتیب وقتی گوشی را به تنظیمات اولیه برمی‌گردانید، کلید رمزگذاری گم می‌شود و خواندن همه داده‌های پاک‌نشده غیرممکن خواهد شد.

امنیت ابتدایی را روی گوشی‌ها اعمال کنید

تمهیداتی برای تامین امنیت گوشی‌ها وجود دارند که در هر شرایطی مهم و کاربردی‌اند؛ هم در شرایطی که اینترنت قطع است و قصد مستندسازی دارید، هم در هر شرایط دیگری. در اینجا به منابع دیگری از سازمان‌های دیگر لینک داده‌ایم:

- Security in a Box
- Electronic Frontier Foundation
- Digital First Aid
- Association for Progressive Communications
- Rory Peck Trust
- Freedom of the Press Foundation (Security)
- Freedom of the Press Foundation (Police)

حتما می‌دانید که هیچ ابتکاری نمی‌تواند امنیت صددرصد را تضمین کند، اما به هر حال به بعضی از راهکارهای کلیدی اشاره می‌کنیم:

- مطمئن شوید که محتوای گوشی‌تان رمزگذاری شده است. رمزگذاری روی گوشی‌های جدیدتر به صورت پیش‌فرض فعال است. اگر در مورد وضعیت رمزگذاری گوشی‌تان مطمئن نیستید، بخش تنظیمات امنیتی گوشی‌تان را چک کنید.
- سیستم عامل گوشی‌تان را مرتب به‌روزرسانی (آپدیت) کنید. با به‌روزرسانی مرتبا، بسیاری از حفره‌های امنیتی برطرف می‌شوند.
- اپلیکیشن‌های مهم موجود روی گوشی‌تان (از جمله اپلیکیشن‌های پیام‌رسانی) را مرتبا آپدیت کنید.
- برای گوشی‌تان رمزعبور محکمی بگذارید که دست‌کم از ۶ عدد تشکیل شده است و امکان ورود با لمس انگشت یا اسکن چهره را در آن غیرفعال کنید.
- برای صفحه گوشی‌تان تایمر قفل شدن بگذارید تا در صورتی که بیش از چند دقیقه بی‌استفاده ماند، به صورت خودکار قفل شود.

- سرویس‌های مرتبط با موقعیت مکانی (Location Services) و پیشینه موقعیت‌های مکانی را غیرفعال کنید. گزینه‌های مرتبط با اسکن بلوتوث و وای‌فای را هم غیرفعال کنید. وضعیت دسترسی به موقعیت مکانی را برای هر یک از اپلیکیشن‌هایی که روی گوشی دارید هم بررسی کنید.
- وقتی به بلوتوث یا وای‌فای نیازی ندارید، حتما آن‌ها را غیرفعال کنید تا از رهگیری احتمالی گوشی‌تان پیش‌گیری کنید.
- وقتی به گوشی‌تان نیاز ندارید، خاموشش کنید.

اپلیکیشن‌های مفیدِ مستندسازی را نصب کنید

برای ثبت عکس و ویدئو می‌توانید از اپلیکیشن‌های پیش‌فرض موجود روی گوشی‌تان یا از اپلیکیشنی که در زمینه مستندسازی کمی تخصصی‌تر کار می‌کند - مثل ProofMode - استفاده کنید که هم امکان ثبت و استخراج داده‌ها و فراداده‌ها را فراهم می‌کند، هم امکانات دیگری نظیر تایید هویت، رمزگذاری و گالری‌های امن را دارد.

یکی از اپلیکیشن‌های مفید در زمان خاموشی اینترنت OONI Probe است که اپلیکیشنی متن‌باز (open-source) است و با اجرا روی گوشی شما به‌طور مستمر وب‌سایت‌ها و پلتفرم‌های فیلترشده را چک می‌کند. این اپلیکیشن می‌تواند به شما نشان دهد که سایت‌ها کجا، کی، چگونه و از سوی چه کسانی فیلتر می‌شوند. لطفا پیش از استفاده از این اپلیکیشن مطمئن شوید که به خطرات احتمالی آن آگاهی پیدا کرده‌اید.

هنوز مطمئن نیستید که از چه اپلیکیشن‌هایی برای مستندسازی استفاده کنید؟ اینجا در راهنمای آموزشی‌مان به برخی سوالات راهگشا پاسخ داده‌ایم.

بعضی از اپلیکیشن‌های روزمره را نصب کنید

این‌که روی گوشی خود داده‌های محدودی داشته باشید اما از چند اپلیکیشن تخصصی استفاده کنید، می‌تواند شک‌برانگیز باشد. برای این‌که گوشی شما یک گوشی معمولی به نظر برسد، چند اپلیکیشن معمولی روزمره را هم نصب کنید که استفاده از آن‌ها در محل زندگی‌تان رایج است (حتما آن‌ها را از منابع معتبر دانلود کنید) و برای عادی نشان دادن گالری عکس‌هایتان هم چند عکس بی‌خطر بگیرید و در آن ذخیره کنید.

برای اپلیکیشن‌های شبکه‌های اجتماعی، شاید بهتر باشد که حساب‌های کاربری جدیدی ایجاد کنید و روی گوشی‌تان به آن‌ها وصل باشید. البته باید به خاطر داشته باشید که ایجاد حساب‌های جعلی، تخطی از قوانین این پلتفرم‌ها محسوب می‌شود و شرایط تایید هویت در برخی از این پلتفرم‌ها هم ایجاد حساب‌های جعلی را دشوار می‌کند. گذشته از این‌ها، شما باید زمان قابل توجهی را صرف تولید محتوا و افزودن دوستان در این حساب‌های جدید بکنید، که می‌تواند پرزحمت باشد.

نصب کردن اپلیکیشن‌ها وقتی اینترنتی وجود ندارد

بدیهی است که دانلود و نصب اپلیکیشن‌ها وقتی دسترسی به اینترنت وجود ندارد، دشوار است. اگر احتمال خاموشی اینترنت می‌رود، باید اپلیکیشن‌های مورد نیازتان را پیش از قطعی اینترنت دانلود کنید.

یک استراتژی که می‌تواند به شما و دیگران پس از قطعی اینترنت هم کمک کند این است که بسته اندرویدی (.apk) مرتبط با اپلیکیشن‌ها را از منابع معتبر دانلود کنید و آن را روی حافظه گوشی یا فلش مموری داشته باشید. داشتن این فایل‌های APK به صورت آفلاین به شما این امکان را می‌دهد که در هنگام خاموشی اینترنت هم بتوانید آن را با دیگران به اشتراک بگذارید.

اگرچه خودمان هنوز فرصت امتحان کردن آن را نداشته‌ایم، اما اپلیکیشن F-Droid رابطی برای مبادله فایل‌های APK به صورت آفلاین ارائه می‌کند. از این‌جا می‌توانید راهنمای آن را ببینید.

اطلاعات شخصی واقعی یا حساس خود را روی گوشی نگه ندارید

سعی کنید از این گوشی‌تان فقط برای مستندسازی استفاده کنید. برای ایمیل، تماس‌های تلفنی یا پیام‌رسانی به دوستان‌تان یا کنشگرانی که می‌دانید ممکن است در معرض خطر قرار گیرند، از این گوشی استفاده نکنید. گوشی مختص مستندسازی را به هیچ‌یک از حساب‌های واقعی و اصلی خود وصل نکنید.

از این امکانات برای پنهان کردن محتوا استفاده کنید

اگر کسی قصد بازرسی شما و گوشی‌تان را دارد، شاید بهتر باشد اهداف واقعی خود را پنهان کنید و یافتن محتوای موجود در گوشی را دشوارتر کنید. در شرایطی که قرار است گوشی شما به صورت سریع و دم‌دستی مورد بازرسی قرار گیرد، می‌توانید از این تاکتیک‌ها استفاده کنید:

- نام و آیکون‌های میان‌بری که برای دسترسی به اپلیکیشن‌ها روی گوشی‌تان وجود دارد را با استفاده از یک اپلیکیشن لانچر مانند Nova Launcher تغییر دهید.
- از یکی از امکانات حریم خصوصی که روی گوشی وجود دارد استفاده کنید. مثلا Private Mode برای گوشی‌های سامسونگ و Content Lock برای گوشی‌های الجی.
- قرار دادن فایلی خالی با نام ".nomedia" درون هر فولدری، جلوی ورود محتوای آن فولدر به بخش «گالری» را خواهد گرفت. اگر حتی پس از قرار دادن این فایل، همچنان محتوای فولدر در گالری‌تان نمایش داده می‌شود، باید Gallery cache را پاک‌سازی کنید. این ترفند ممکن است روی همه گوشی‌ها به یک شکل کار نکند.

شما می‌توانید با استفاده از یک اپلیکیشن مدیریت فایل، فولدرهای مخفی ایجاد کنید. فولدرهایی که نام‌شان با نقطه (.) شروع می‌شود، مخفی خواهند بود. انتقال فایل به این فولدرهای مخفی را یا خودتان باید انجام دهید یا اگر از یک اپلیکیشن تصویربرداری نظیر Open Camera استفاده می‌کنید، می‌توانید در تنظیمات اپلیکیشن مسیر ذخیره‌سازی آن را مشخص کنید. مطمئن شوید که گزینه Show Hidden Files را در بخش تنظیمات غیرفعال کرده‌اید تا فایل‌های مخفی نمایش داده نشوند.

برخی از اپلیکیشن‌های تخصصی مستندسازی، مانند Tella یا Eyewitness to Atrocities محتوا را فقط در گالری‌های رمزگذاری‌شده جداگانه‌ای که محتویات آن فقط از درون اپلیکیشن قابل دسترسی است، ذخیره کنید. چنین اقدامی می‌تواند دسترسی به آن‌ها را برای کسانی که گوشی‌تان را بازرسی می‌کنند، دشوارتر کند. ذخیره‌سازی محتوا در این «گالری‌های امن» نیازمند یک رمز عبور جداگانه است تا حتی وقتی گوشی‌تان قفل نیست هم محتویات آن رمزگذاری‌شده بمانند.

نکات مهمی درباره پنهان کردن محتویات گوشی

لطفا در نظر داشته باشید که تکنیک‌هایی که پیش‌تر به آن‌ها اشاره کردیم شاید برای رها شدن از دست کسی که وقت زیادی صرف بازرسی گوشی‌تان نمی‌کند کافی باشد، **اما نمی‌تواند به‌طور موثری محتویات گوشی‌تان را از چشم کسی که مصمم است داده‌های مخفی شما را بیابد، دور نگه دارد.**

این نکته را هم مد نظر داشته باشید که برخی از کشورها ممکن است قوانینی برای محدود کردن استفاده از اپلیکیشن‌های امنیتی مرتبط با رمزگذاری یا پاک‌سازی داده‌ها داشته باشند یا حتی آن را تحت پیگرد قضایی قرار دهند. در چنین شرایطی، استفاده از این اپلیکیشن‌ها و ترفندها، ممکن است از نگاه مقام‌های مسئول «تلاش برای از بین بردن شواهد» یا «مخدوش کردن روند تحقیقات» تلقی شود و جرمی قابل پیگرد باشد. اگر درباره قوانین مرتبط با این موضوع در کشورتان سوالی دارید، این نقشه جامع (مربوط به سال ۲۰۱۷) می‌تواند نقطه شروع خوبی باشد.

راه‌اندازی امکان به‌اشتراک‌گذاری (همرسانی) آفلاین

ممکن است پس از ثبت و ضبط تصاویر به اینترنت دسترسی نداشته باشید، اما همچنان بخواهید بخشی از این داده‌ها را از گوشی‌تان خارج کنید؛ به دلایل امنیتی، یا برای آزاد کردن فضا در صورت محدود بودن حافظه، یا به هدف به‌اشتراک‌گذاری با دیگران. خالی کردن مرتب گوشی به شما کمک می‌کند که میزان اطلاعات بربادرفته یا لو رفته در صورت ضبط و مصادره گوشی‌تان را به حداقل برسانید.

حتی اگر نمی‌توانید به اینترنت وصل شوید، همچنان می‌توانید به صورت محلی با وای‌فای یا بلوتوث به دستگاه‌های دیگری متصل شوید، مثلا یک گوشی دیگر یا یک درایو USB متصل به وای‌فای. معمولا گوشی‌ها اپلیکیشن یا رابطی برای اتصال و انتقال داده‌ها دارند. اگر گوشی شما هم چنین امکانی را فراهم می‌کند، می‌توانید یک USB در حرکت (OTG) را هم به آن وصل کنید تا محتویات گوشی به درایو OTG یا یک دستگاه دیگر منتقل شود.

درباره جزئیات این روش‌ها در دو راهنمای «به‌اشتراک‌گذاری و برقراری ارتباطات در هنگام خاموشی اینترنت» و «ویدئو به مثابه شاهد: ابزارهای فنی و انتقال فایل‌ها» به تفصیل گفته‌ایم.

پیش از آن‌که در شرایط بحرانی قرار بگیرید، تمرین کنید

اگر به اینترنت دسترسی دارید، همین حالا گوشی‌تان را آماده کنید. سعی کنید با استفاده هر روزه از اپلیکیشن‌ها، بهره‌گیری از آن‌ها را در شرایطی که هیچ نگرانی امنیتی وجود ندارد، تمرین کنید. به این ترتیب با زیر و بم کار آشنا خواهید شد و استفاده از این اپلیکیشن‌ها برای شما آسان خواهد شد. کاری کنید که اصول پایه‌ی امنیت، روال معمول و پیش‌فرض شما باشد. در این صورت وقتی در موقعیتی بحرانی قرار گرفتید که دغدغه‌های دیگری را هم ممکن است با خود به همراه بیاورد، همه کارهای لازم را به سادگی انجام خواهید داد.

پست بعدی مجموعه را ببینید: آیا باید از این اپلیکیشن مستندسازی استفاده کنم؟

****

آیا باید از این اپلیکیشن مستندسازی استفاده کنم؟

اپلیکیشن‌های بسیاری وجود دارند که می‌توانید از آن‌ها برای ثبت تصاویر ویدئویی استفاده کنید؛ از اپلیکیشن دوربین پیش‌فرض گوشی گرفته تا اپلیکیشن‌های تخصصی‌تری مثل ProofMode و Tella و Eyewitness to Atrocities که برخی از آن‌ها امکاناتی دارند که فقط با دسترسی به اینترنت فراهم می‌شوند. بنابراین به خاطر داشته باشید که برخی از امکانات این اپلیکیشن‌ها در زمان خاموشی اینترنت ممکن است قابل استفاده نباشند.

ما نمی‌توانیم بگوییم که مشخصا کدام اپلیکیشن برای شما مناسب‌تر است، چون پاسخ به این سوال کاملا بستگی به موقعیت شما، نیازهایتان و خطراتی دارد که با آن‌ها مواجه‌اید. (برای درک بهتر «ارزیابی خطرات و تهدیدها» می‌توانید به این پست وبلاگی مراجعه کنید.)

وقتی ارزیابی خطرات و تهدیدها را انجام دادید، با سوالات راهگشایی که در ادامه آمده می‌توانید ببینید کدام اپلیکیشن مستندسازی تصویری، بهتر از دیگران به کارتان می‌آید.

چه کسانی این اپلیکیشن را ساخته‌اند و آیا من به آن‌ها اعتماد دارم؟

همیشه باید توجه ویژه‌ای به سازندگان اپلیکیشن‌هایی که روی گوشی و سیستم‌های دیگر دانلود و نصب می‌کنید داشته باشید. آیا به آن‌ها اعتماد می‌کنید که شما را خواسته یا ناخواسته در معرض خطر قرار ندهند؟

در این‌جا نکاتی آمده که باید مد نظر قرار دهید:

- آیا سازندگان این اپلیکیشن خوش‌نامند؟ آدم‌های دیگری که در شبکه و گروه‌تان دارید درباره آن‌ها و ابزارهایی که ساخته‌اند چه می‌گویند؟
- آیا سازندگان این اپلیکیشن‌ها آسیب‌پذیرند؟ در نظر داشته باشید که با توجه به موقعیتی که دارند، تا چه اندازه ممکن است راضی به تحویل داده‌های شما شوند یا با ایجاد «در پشتی» به مقام‌های مسئول امکان دسترسی به داده‌های کاربران را بدهند و اینکه تابه‌حال این کار را کرده‌اند یا خیر؟
- داده‌های کاربران این اپلیکیشن در کدام کشورها ذخیره می‌شوند و در حوزه قضایی آن کشورها چه قوانینی درباره حراست از داده‌ها یا تحویل آن‌ها وجود دارد؟
- آیا مسئولیت نگه‌داری اپلیکیشن هم با سازندگان آن است؟ اگر آن‌ها مسئول نگه‌داری نباشند، احتمال هک شدن و نفوذ به آن‌ها با هدف قرار گرفتن حفره‌های امنیتی، افزایش می‌یابد. وب‌سایت سازندگان اپلیکیشن یا صفحه اپلیکیشن در گوگل‌پلی را چک کنید و ببینید آخرین نسخه آپدیت‌شده این اپلیکیشن مربوط به چه تاریخی است؟
- سازنده یا سازندگان اپلیکیشن تا چه اندازه در کار خود جاافتاده‌اند و آیا می‌توانند این اپلیکیشن را در طول زمان پایدار نگه دارند؟
- آیا این اپلیکیشن متن‌باز (open-source) است؟ احتمال کشف و رفع مشکلات امنیتی احتمالی در اپلیکیشن‌های متن باز بالاتر است چون موشکافانه می‌شوند. آیا سازندگان اپلیکیشن درباره کارآمدی و امنیت آن شفافیت دارند؟
- سازندگان اپلیکیشن چه انگیزه‌ها و مشوق‌هایی برای کارشان دارند و این انگیزه‌ها و مشوق‌ها چه تاثیری بر اعتبار آن‌ها دارند؟ مثلا آیا آن‌ها ماموریت ویژه‌ای دارند؟ به دنبال کسب سود هستند؟ از حمایت سرمایه‌گذاران خاصی برخوردارند؟
- اگرچه همواره نمی‌تواند نشانه مستقیمی در تایید اعتبار یک اپلیکیشن باشد، هزینه استفاده از یک اپلیکیشن می‌تواند نکته مهمی باشد که باید مد نظر داشت. برخی اپلیکیشن‌ها هزینه اشتراک بالایی دارند یا بابت هر ویدئو مبلغی از کاربر می‌گیرند.

برای دریافت اطلاعات بیشتر درباره دفاع شخصی در برابر تجسس به راهنمای EFF مراجعه کنید.

این اپلیکیشن از کجا قابل دانلود است؟

شما همواره باید اپلیکیشن‌های مورد استفاده خود را از وب‌سایت‌ها یا منابع معتبر دانلود کنید. حتی اگر درباره اعتبار و امنیت یک اپلیکیشن مشخص تحقیقات جامعی انجام داده‌اید، اپ‌استورهای مرموز همچنان ممکن است فریب‌تان دهند و نسخه‌های جعلی اپلیکیشن‌ها را در برابرتان بگذارند که اهداف مخربی دارند. به عنوان مثال، سال گذشته یک سازمان فعال در زمینه حقوق دیجیتال به نام SMEX هشدار داد که برخی وب‌سایت‌های مشکوک مشغول بازاریابی برای اپلیکیشنی به نام «واتس‌اپ پلاس» هستند (برای شفاف‌سازی باید تاکید کنیم که واتس‌اپ پلاس محصول واتس‌اپ نیست) که به طور بالقوه ممکن است مشغول ذخیره‌سازی و فروش داده‌های کاربران باشد یا گوشی‌هایی که این اپلیکیشن روی‌شان نصب شده را در معرض حملات هکرها قرار دهد.

برخی از برنامه‌نویسان و اپلیکیشن‌سازانی که دغدغه امنیت دارند حتی کلیدهای رمزگذاری‌شده‌ای در اختیار کاربران قرار می‌دهند که با بهره‌گیری از آن‌ها می‌توان اصالت اپلیکیشن‌ها را بررسی کرد. آن‌ها معمولا راهنمایی هم برای شرح چگونگی بررسی و تایید این امضاهای دیجیتال ارائه می‌کنند..

داده‌های شما کجا ذخیره می‌شوند؟

برخی از اپلیکیشن‌های مستندسازی، داده‌های شما را فقط روی گوشی خودتان ذخیره می‌کنند، در حالی که بعضی دیگر علاوه بر گوشی، داده‌های کاربر را در جایی دیگر هم ذخیره می‌کنند. در بیشتر موارد این بستگی به طراحی و اهداف اپلیکیشن مورد نظر دارد. مثلا اپلیکیشن Eyewitness to Atrocities یک کپی از تصاویر را به یک پایگاه ذخیره‌سازی به نام Lexis Nexis می‌فرستد تا سازندگان آن بتوانند زنجیره مالکیت فایل‌ها و اصالت محتوای آن‌ها را تایید کنند. شما فقط در صورتی می‌توانید تصاویر و فایل‌های چندرسانه‌ای را از گالری رمزگذاری‌شده درون این اپلیکیشن خارج کنید که پیش از آن - برای حراست از موجودیت و امنیت فایل‌ها - در سرورهای Lexis Nexis ذخیره شده باشد.

این کاملا به شما و کارتان بستگی دارد که مشخص کنید می‌خواهید تصاویری که ثبت کرده‌اید فقط روی گوشی‌تان ذخیره شود یا می‌خواهید آن را جایی دور از دسترس که در کنترل خودتان است هم ذخیره کنید (امکانی که اپلیکیشن Tella فراهم می‌کند) یا حتی شاید بخواهید آن را برای سازمان یا پلتفرم مشخصی هم بفرستید که پیش‌تر اجازه دسترسی و استفاده از تصاویر را به آن‌ها داده‌اید. به خاطر داشته باشید که در زمان قطعی اینترنت نمی‌توانید بلافاصله آن‌چه ثبت کرده‌اید را برای کسی یا جایی بفرستید، بنابراین به اپلیکیشنی نیاز دارید که دست‌کم به صورت موقت امکان ذخیره‌سازی محلی (و ترجیحا تهیه نسخه بک‌آپ) را هم به شما بدهد. (برای دریافت اطلاعات بیشتر درباره بک‌آپ گرفتن یا همان نسخه پشتیبانی از موبایل بدون دسترسی به اینترنت، این راهنما را بخوانید.)

اگر داده‌های شما قرار است در جای دیگری هم ذخیره شود، باید اطلاعات لازم درباره کشورهای میزبان را کسب کنید. این داده‌ها در آن کشورها تا چه اندازه آسیب‌پذیرند؟ چه در برابر احکام دادگاهی چه از راه‌های دیگر. اگر داده‌های شما در آن کشورها لو برود چه خطراتی متوجه شما خواهد بود؟ این سوالاتی است که باید پیش از ذخیره‌سازی داده‌ها، پاسخ‌شان را داشته باشید.

آیا این اپلیکیشن تصاویر من را رمزگذاری می‌کند؟

بعضی اپلیکیشن‌ها مثل Tella و Eyewitness Atrocities امکان رمزگذاری فایل‌ها یا ذخیره‌سازی رمزگذاری‌شده محتوا را فراهم می‌کنند که مستقل از گالری اصلی گوشی و متد رمزگذاری آن است. دلیلش این است که داده‌ها و فراداده‌ها

(Metadata) هرگز بدون رمزگذاری نمانند مگر در شرایطی که از درون اپلیکیشن و با وارد کردن رمز عبور به آن دسترسی پیدا کنید. به عبارت دیگر یعنی حتی اگر قفل گوشی‌تان باز باشد، اپلیکیشن مستندسازی شما رمزگذاری‌شده باقی خواهد ماند. به این ترتیب سطح بالاتری از امنیت برای اپلیکیشن مستندسازی شما فراهم می‌شود.

اگر تنظیمات اپلیکیشن شما به‌گونه‌ای است که به محض بازیابی دسترسی به اینترنت فایل‌های تصویری شما را به مکانی دیگر منتقل و در آن‌جا ذخیره می‌کند، این نکته را هم مد نظر قرار دهید که فایل‌ها در زمان انتقال و نیز در زمان ذخیره شدن در مکان دیگر، رمزگذاری‌شده می‌مانند یا نه. به عنوان مثال، اپلیکیشن EyeWitness این امکان را فراهم می‌کند.

این نکته را هم به خاطر داشته باشید که اگرچه در بسیاری از نقاط جهان رمزگذاری کاملا قانونی است، بعضی کشورها ممکن است آن را محدود کنند یا حتی تحت پیگرد قضایی قرار دهند. این نقشه (بر اساس اطلاعات سال ۲۰۱۷) نقطه آغاز خوبی برای پاسخ‌گویی به سوالات‌تان درباره قوانین مرتبط با رمزگذاری در کشورهای گوناگون است.

آیا این اپلیکیشن فراداده‌های مهم را هم (بدون دسترسی به اینترنت) ثبت می‌کند؟

فراداده (Metadata) داده‌ای است که اطلاعات عکس یا ویدئوی شما را تشریح می‌کند: زمان، تاریخ و موقعیت مکانی ثبت تصاویر، همه در فراداده ذخیره می‌شوند. این اطلاعات برای تشخیص، درک و تایید هویت و صحت‌سنجی عکس یا ویدئویی که به عنوان مدرکی از رویداد خاصی تهیه شده، بسیار ارزشمند است. در شرایط خاموشی اینترنت، توانمندی یک اپلیکیشن برای جمع‌آوری فراداده‌های خاص به صورت اتوماتیک و یا میسر کردن امکان اضافه کردن آسان اطلاعات توصیفی مرتبط با مکان، بسیار مفید است؛ به این خاطر که در صورت قطعی اینترنت ممکن است شما برای مدتی طولانی نتوانید آنچه مستند کرده‌اید را با کسی هم‌رسان کنید (و در این بازه زمانی ممکن است جزئیات مرتبط با شرایط موجود در لحظه را از یاد ببرید).

اکثر اپلیکیشن‌های تخصصی مستندسازی مانند ProofMode ویژگی‌های تقویت‌شده‌ای برای ثبت فراداده‌ها دارند و فراداده‌هایی که جمع‌آوری و ثبت می‌کنند نسبت به آن‌چه در اپلیکیشن‌های دوربین پیش‌فرض روی گوشی‌ها ثبت می‌شوند، به طور چشم‌گیری بیش‌تر است. فراداده‌های تقویت‌شده می‌توانند داده‌های مرتبط با حسگر دوربین‌ها، سیگنال‌های بلوتوث یا وای‌فای موجودِ پیرامون، داده‌های مرتبط با دستگاه ثبت‌کننده، الگوریتم رمزگذاری و اطلاعات فراهم‌شده از سوی کاربر را در بر بگیرند. همه این موارد به تایید هویت و صحت‌سنجی ویدئو در آینده کمک می‌کنند.

این نکته را به خاطر داشته باشید که در شرایط خاموشی اینترنت، شما به اپلیکیشنی نیاز دارید که برای تولید یا ثبت فراداده‌ها، لزوما نیازی به انتقال داده‌ها نداشته باشد. برخی اپلیکیشن‌ها ممکن است به جای حسگرهای سخت‌افزاری، متکی به اینترنت باشند تا بتوانند فراداده‌های خاص را گردآوری و ثبت کنند. به عنوان مثال، اگر داده‌های مرتبط با موقعیت مکانی از روی دستگاه ثبت شده باشند، فراداده‌ها ممکن است فقط آخرین موقعیت مکانی که اتصال اینترنتی دستگاه برقرار بوده را نشان دهند، به جای این‌که موقعیت مکانی درست و واقعی سخت‌افزار را نشان دهند. در حالت ایده‌آل، اپلیکیشن مستندسازی شما باید این قابلیت را داشته باشد که بتوانید فراداده‌ها را به‌صورت محلی و بدون دسترسی به اینترنت هم ذخیره کنید (مانند Offline Mode در اپلیکیشن Tella) و همه فرم‌های موجود را هم ذخیره کند.

آیا می‌توانم از داده‌های موجود روی اپلیکیشن، خروجی بگیرم؟

بسته به این‌که هدف‌تان از مستندسازی چه باشد، ممکن است قابلیت خروجی گرفتن از مستندهای ویدیویی و فراداده مرتبط با آن در اپلیکیشن، برای کارتان حیاتی باشد، آن هم در فرمتی که مختص آن اپلیکیشن خاص نیست. یعنی باید بتوانید این فایل‌های رسانه‌ای و فراداده‌ی آن را در محیط‌های خارج از این اپلیکیشن هم باز کنید و ببینید.

قابلیت خروجی گرفتن یعنی این‌که شما و دیگران برای دسترسی به فایل‌های مستند شده، وابسته به یک اپلیکیشن خاص نیستید و این برای مراحل آینده و کار روی محتوا امکانات بیش‌تری به شما می‌دهد.

این نکته را هم در ذهن داشته باشید که برخی از فراداده‌ها ممکن است بدون دسترسی به پایگاه‌های داده خاص یا نمودارهای تبدیل فرمت برای تفسیر اعداد، قابل خواندن نباشند. (به عنوان مثال، در مورد شناسه‌های برجک‌های موبایل یا شبکه‌های وای‌فای).

این نکته را هم در نظر داشته باشید که برخی از اپلیکیشن‌ها ممکن است زنجیره نگه‌داری از فایل‌ها را بسته نگه دارند و امکان خروجی گرفتن را به کاربران ندهند و حتی در بعضی دیگر از اپلیکیشن‌ها امکان خروجی گرفتن از ابتدا در ذهن طراحان‌اش نبوده باشد.

این نکته را هم باید بدانید که برخی اپلیکیشن‌ها مانند Eyewitness و Atrocities ممکن است تا زمانی که فایل‌تان را روی یک سرور دور از دسترس آپلود نکرده‌اید، امکان خروجی گرفتن را به شما ندهند (که برای انجام چنین کاری طبعا نیاز به دسترسی به اینترنت دارید) و برخی اپلیکیشن‌ها هم اگرچه امکان خروجی گرفتن از فایل‌های رسانه‌ای را می‌دهند، این امکان را برای فراداده‌ها غیرفعال کرده‌اند (به غیر از فراداده‌ای که در دل فایل‌ها موجود است).

اگر نیاز به خروجی گرفتن دارید، در حالت ایده‌آل اپلیکیشن شما باید امکان تهیه یک نسخه خروجی بدون هیچ‌گونه تغییر و تحول را بدهد و همین‌طور یک کپی از فراداده در فرمت متنی خوانا و استاندارد.

به عنوان مثال فراداده‌های اپلیکیشن Tella در گالری این اپلیکیشن به صورت رمزگذاری‌شده ذخیره می‌شود، اما می‌توان خروجی در فرمت CSV هم از آن گرفت.

گذشته از این، در هنگام خاموشی اینترنت، لازم است بتوانید گزینه‌هایی برای خروجی گرفتن به اپلیکیشن‌های آفلاین یا دیگر سرویس‌های مستقل از اینترنت هم داشته باشید. بیشتر اپلیکیشن‌ها نوعی از همرسانی را با تعبیه دکمه‌ای نظیر Share فراهم می‌کنند که با کلیک روی آن منوی همرسانی باز می‌شود؛ که در ابزارهای اندرویدی به فهرستی از اپلیکیشن‌هایی می‌رسد که می‌توانند آن فرمت خاص از داده‌ها را باز کنند.

متاسفانه توسعه‌دهندگان اپلیکیشن‌ها می‌توانند منوی همرسانی خود را به دلخواه تغییر دهند و به همین خاطر میان اپلیکیشن‌ها لزوما هماهنگی وجود ندارد.

برای حجم‌های بزرگ‌تری از داده، ممکن است راه‌حل بهینه این باشد که از طریق یک اپلیکیشن مدیریت فایل (File Manager) به فایل‌های ذخیره شده دسترسی داشته باشید، اگرچه با این روش ممکن است نتوانید به فراداده ذخیره شده در پایگاه داده آن اپلیکیشن دسترسی داشته باشید. همچنین، این گزینه برای اپلیکیشن‌هایی که راهکار خودشان را برای دسترسی به «گالری‌های امن» فراهم می‌کنند، وجود ندارد، چرا که فایل‌ها به صورت رمزگذاری‌شده ذخیره می‌شوند. برای چنین اپلیکیشن‌هایی لازم است که قابلیت همرسانی (Sharing) درون اپلیکیشن تعبیه شود.

پست بعدی مجموعه را ببینید: نگه‌داری تصاویر قابل تایید در زمان خاموشی اینترنت

****

نگه‌داری تصاویر قابل تایید در زمان خاموشی اینترنت

مدافعان حقوق بشر، کاوشگران و پژوهشگران و روزنامه‌نگاران، عموما به گزارش‌های مستند دست اولی متکی‌اند که به دست شاهدان عینی تصویربرداری شده است، تا بتوانند رسالت نظارت و گزارشگری خود را به انجام برسانند و موارد نقض حقوق بشر را مستند کنند. آن‌ها برای حصول اطمینان از این‌که بر اساس اطلاعات درست و دقیق اقدام می‌کنند، قدم‌هایی برمی‌دارند که سنجش اصالت و تایید صحت مستندات دریافتی‌شان را ممکن می‌سازد؛ فرآیندی که می‌تواند بسیار پرزحمت و زمان‌بر باشد.

به عنوان فردی که مستندسازی می‌کند، اقدامات ساده‌ای وجود دارند که شما با انجام آن‌ها می‌توانید فرآیند درستی‌سنجی فایل‌ها و مستندات خود را برای دیگران ساده‌تر کنید، تا بتوان به موقع و به شیوه‌ای موثر از آن استفاده کرد. این قدم‌های مهم در زمان خاموشی اینترنت اهمیت بیش‌تری می‌یابند.

این موارد را در نظر بگیرید:

- اگر نتوانید بلافاصله فایل‌های خود را آپلود کنید، تاریخ انتشار و اطلاعات موقعیت مکانی منتشر شده در شبکه‌های اجتماعی نمی‌تواند کمکی به سنجش اصالت بکند و تایید کند که ویدئوی شما در روز مشخصی یا پیش از آن یا در موقعیت مکانی خاصی تصویربرداری شده است.
- اگر دیگران هم نتوانند فایل‌های خود را آپلود کنند، ممکن است در مجموع تعداد فایل‌های مستند موجود که می‌تواند راهی برای تایید اصالت ویدئوی شما باشد هم کم باشد.
- اگر لازم باشد ویدئوی خود را چندین بار دست به دست کنید تا به مقصد نهایی برسد، ممکن است رهگیری منبع ویدئو برای دیگران دشوارتر شود.
- اگر لازم باشد که ویدئوی اصلی را از روی گوشی‌تان به دلایل امنیتی یا کمبود حافظه دستگاه بدون آن‌که نسخه پشتیبان (بک‌آپ) آن را روی کلاود قرار داده باشید حذف کنید، یا اگر لازم شود که از شر موبایل‌تان خلاص شوید، تایید اصالت ویدئو احتمالا دشوارتر خواهد شد.
- اگر جزئیات مرتبط با ویدئویی خاص را فراموش کنید یا اپلیکیشنی که از آن بهره می‌گیرید بدون دسترسی به اینترنت قادر به ذخیره‌سازی فراداده‌ها نباشد، دیگران ممکن است در تایید اصالت آن با مشکلاتی مواجه شوند.

ترفندهایی که در ادامه آورده‌ایم به شما کمک خواهند کرد تا در جریان خاموشی اینترنت بتوانید از ویدئوی خود حراست کنید تا قابلیت درستی‌سنجی و کارکرد آن به عنوان یک فایل مستند در آینده، حداکثری باشد.

جزئیات کمک‌کننده به تایید اصالت ویدئو را فراهم کنید یا از آن‌ها تصویربرداری کنید

تلاش کنید جزئیاتی را در ویدئوی خود بگنجانید تا کار پژوهشگران و روزنامه‌نگاران را در آینده برای تایید اصالت ویدئو و تشخیص زمان و مکان آن آسان‌تر کند. می‌توانید از مکان‌های شناخته‌شده و افق شهر و نشانه‌های خیابان‌ها و پلاک ماشین‌ها، ورودی مغازه‌ها، پرچم‌ها و ساعت‌ها و صفحات روزنامه‌ها برای این منظور استفاده کنید. شما همچنین می‌توانید اطلاعات پایه نظیر نام و اطلاعات تماس خودتان (در صورت امن بودن چنین کاری) و ساعت، تاریخ و اطلاعات جی‌پی‌اس و موقعیت مکانی را روایت کنید، یا این‌که این‌ها را روی تکه کاغذی بنویسید و از آن فیلم بگیرید. هرچه جزئیاتی که فراهم می‌کنید بیش‌تر باشد، کار کسی که می‌خواهد اصالت ویدئو را تایید کند حتی اگر شما را نشناسد یا نداند

ویدئو از کجا آمده است، آسان‌تر خواهد شد. نکات مرتبط با بهترین روش‌ها در ثبت، ضبط، ذخیره‌سازی و همرسانی را از این‌جا ببینید.

توصیف و توضیح / فراداده اضافه کنید

از یکی از اپلیکیشن‌های فراوان مستندسازی بهره بگیرید که فراداده پیشرفته را ثبت می‌کنند و اطلاعات فنی را از روی گوشی شما می‌گیرند و به شما این امکان را هم می‌دهند که بتوانید توضیحات تکمیلی خود را به آن بیفزایید. این نکته را مد نظر داشته باشید که در جریان خاموشی و قطعی اینترنت، شما به اپلیکیشنی نیاز دارید که برای ضبط و ذخیره‌سازی فراداده نیازی به دسترسی به اینترنت نداشته باشد. برای اطلاعات بیش‌تر درباره نحوه انتخاب اپلیکیشن مناسب، می‌توانید مطلب «آیا باید از این اپلیکیشن مستندسازی استفاده کنم؟» را مطالعه کنید.

حتی اگر از اپلیکیشنی تخصصی برای مستندسازی استفاده نمی‌کنید هم می‌توانید اطلاعات تکمیلی را به شکل یادداشت، نقشه یا عکس به موبایل‌تان اضافه کنید. با استفاده از اپلیکیشن مدیریت فایل دلخواه خود می‌توانید ویدئوها را مرتب کنید و اطلاعات تکمیلی را به آن بیفزایید.

مهم‌ترین اطلاعات تکمیلی یک ویدئو، زمان تصویربرداری، مکانی که واقعه در آن رخ داده و منبع آن است (که می‌تواند نام و اطلاعات تماس خودتان باشد، در صورتی که اضافه کردن آن امنیت‌تان را به خطر نیندازد).

فراداده را استخراج کنید و آن را به همراه ویدئو (که می‌توانید همه آن‌ها را در یک فایل زیپ قرار دهید) سپس با شخص یا اشخاصی که می‌خواهید به اشتراک بگذارید.

نسخه پشتیبان (بک‌آپ) تهیه کنید

به صورت منظم از فایل‌های تصویری موجود روی موبایل‌تان، نسخه پشتیبان تهیه کنید. به عنوان مثال می‌توانید درایوهای وایرلس یا OTG را به موبایل‌تان وصل کنید تا حتی بدون دسترسی به کامپیوتر بتوانید بک‌آپ بگیرید. نکته‌هایی که در مطلب «بک‌آپ گرفتن از فایل‌های رسانه‌ای موبایل بدون دسترسی به اینترنت یا کامپیوتر» آورده‌ایم را به دقت مطالعه کنید.

با تهیه بک‌آپ می‌توانید مطمئن باشید که یک کپی از ویدئوهای شما حتی در صورتی که آسیبی به موبایل‌تان وارد شود یا مجبور شوید آن‌ها را از روی گوشی پاک کنید، جایی در دسترس خواهد بود. در اختیار داشتن یک کپی امن از ویدئوی اصلی شما این امکان را به پژوهشگران یا روزنامه‌نگارانی که آن را می‌بینند خواهد داد که بتوانند بعدها اصل ویدئو را از خودتان دریافت کنند (البته اگر بتوانند رد شما را پیدا کنند) و به این ترتیب زنجیره نگه‌داری از فایل کوتاه‌تر و کامل‌تر خواهد بود.

پست بعدی مجموعه را ببینید: بک‌آپ گرفتن از فایل‌های تصویری موجود در موبایل، بدون دسترسی به اینترنت یا کامپیوتر

****

بک‌آپ گرفتن از فایل‌های تصویری موجود در موبایل، بدون دسترسی به اینترنت یا کامپیوتر

تهیه نسخه پشتیبان (بک‌آپ) بسیار اهمیت دارد تا اطمینان حاصل کنید که فایل‌های مستند شما به صورت تصادفی حذف نمی‌شوند و یا در صورت مصادره شدن گوشی شما، از دست نمی‌روند. در زمان خاموشی یا کند شدن شدید اینترنت، ممکن است نتوانید به شیوه‌های معمول خود بک‌آپ بگیرید یا فایل‌های خود را به جای امن دیگری برسانید. کپی کردن این فایل‌ها به یک کامپیوتر یا لپ‌تاپ دیگر یکی از راه‌های بک‌آپ گرفتن است، اما از آن‌جایی که اغلب کاربران به چنین امکانی دسترسی ندارند، در این‌جا نکات و ترفندهایی آورده‌ایم که به شما در تهیه نسخه پشتیبان از فایل‌ها در هنگام خاموشی اینترنت یا زمانی که به کامپیوتری دسترسی ندارید، یاری می‌رسانند.

استفاده از درایو وایرلس یا OTG

درایوهای OTG نوعی از فلش‌های یواس‌بی هستند که با بسیاری از ابزارهای اندرویدی (و نه همه آن‌ها) سازگارند. شما می‌توانید یک درایو OTG را مستقیما به موبایل‌تان وصل کنید یا از مبدل اوتی‌جی به یواس‌بی برای اتصال آن به یک حافظه (هارد) بیرونی استفاده کنید. با اوتی‌جی، موبایل شما برق لازم برای درایو را هم فراهم می‌کند.

از برندهای مشهور درایوهای اوتی‌جی، می‌توان از سان‌دیسک (SanDisk) و کینگستون (Kingston) و سامسونگ نام برد که معمولا قیمتی بین ۸ تا ۲۵ دلار دارند و قیمت آن‌ها بسته به ظرفیت ذخیره‌سازی‌شان متفاوت است.

درایوهای وایرلس هم شبیه هارد درایوهای معمولی‌اند، با این تفاوت که برای استفاده از آن‌ها به کابل نیازی ندارید. به ای. ترتیب می‌توانید ابزارهایی را که به صورت پیش‌فرض به هارد درایوها وصل نمی‌شوند به هارد درایو وصل کنید، از جمله گوشی هوشمندتان. یکی از مزیت‌های درایوهای وایرلس به درایوهای اوتی‌جی این است که همزمان می‌توانید چندین ابزار مختلف را به آن‌ها وصل کنید. این امکان در شرایطی که اعتراضات در جریان است و شما در قالب یک تیم مشغول تصویربرداری هستید، می‌توان کمک بزرگی باشد. یعنی همه ویدئوها می‌تواند روی هاردی که یکی دیگر از اعضای تیم حمل می‌کند، ذخیره شود. این نکته را مد نظر داشته باشید که درایوهای وایرلس با نیروی باتری کار می‌کنند و باید شارژ شوند.

سان‌دیسک احتمالا محبوب‌ترین برند در میان درایوهای وایرلس است، اگرچه برندهای دیگری هم وجود دارند. درایوهای وایرلس معمولا از درایوهای اوتی‌جی گران‌ترند و قیمت‌شان بسته به میزان ذخیره‌سازی از ۲۵ تا ۱۰۰ دلار است. قیمت هاردهایی که حافظه بزرگ‌تری دارند هم بسته به میزان ذخیره‌سازی داده‌ها از ۱۵۰ دلار شروع می‌شوند.

راه‌حل جایگزین: از یک گوشی استفاده‌نشده قدیمی بهره بگیرید

اگر هارد درایو بی‌سیم یا اوتی‌جی در اختیار ندارید اما یک گوشی قدیمی دارید که همچنان کار می‌کند، می‌توانید از آن برای بک‌آپ گرفتن استفاده کنید. تا زمانی که هر دو گوشی شما در مجاورت هم باشند، می‌توانید برای کپی کردن فایل‌های رسانه‌ای از یک گوشی به گوشی دیگر از بلوتوث، وای‌فای دیرکت یا اندروید بیم و ارتباطات کوتاه‌برد ان‌اف‌سی (NFC) استفاده کنید. بلوتوث و وای‌فای دیرکت هر دو مبتنی بر تکنولوژی‌های بی‌سیمی هستند که دو ابزار گوناگون را به هم متصل (Pair) می‌کنند بدون آن‌که نیازی به مسیریاب (روتر) یا اکسس‌پوینت دیگری در میانه باشد. وای‌فای دیرکت برد بالاتری دارد و محدوده گسترده‌تری را پوشش می‌دهد و سرعت انتقال داده‌ها هم در آن بالاتر از بلوتوث است، اما مصرف باتری آن به طور چشمگیری بیش‌تر است. NFC هم برد بسیار کوتاه‌تری دارد (کم‌تر از ۴ سانتی‌متر) و سرعت انتقال داده‌اش هم بسیار پائین‌تر از بلوتوث و وای‌فای دیرکت است، اما سریع‌تر وصل می‌شود و مصرف باتری‌اش بسیار کم‌تر

است و به همین خاطر برای انتقال سریع داده‌ها در سایز پایین وقتی هر دو گوشی یا ابزار را در دست دارید، می‌توانید از آن بهره بگیرید.

در گوشی شما احتمالا بلوتوث تعبیه شده است یا اپلیکیشن‌های مرتبط با NFC و وای‌فای دیرکت روی آن موجودند که امکان همرسانی فایل‌ها با دیگر ابزارهای پیرامون را برای‌تان فراهم می‌کنند. اگر اپلیکیشن Files گوگل روی هر دو دستگاه نصب شده باشد، می‌توانید حتی به صورت آفلاین با استفاده از همین تکنولوژی‌ها فایل‌ها را همرسانی کنید.

نکته مهم: نقطه ضعف اتصال آسانی که با استفاده از این روش‌ها میسر می‌شود این است که این‌گونه ارتباطات امن نیستند. اسکنرهای وای‌فای و بلوتوث می‌توانند به سادگی برای رهگیری موقعیت مکانی شما مورد استفاده قرار گیرند. نفوذگران ممکن است تلاش کنند تا به دستگاه شما متصل شوند، فایل‌های ناخواسته و بدافزار برای‌تان بفرستند یا حتی اگر سیستم‌تان آسیب‌پذیر باشد، کنترل آن را به دست بگیرند. **برای این‌که امن‌تر باشید وقتی از این دستگاه‌ها استفاده نمی‌کنید حتما آن‌ها را خاموش نگه دارید و فقط وقتی به جای امنی می‌رسید آن‌ها را به حالت روشن برگردانید. سطح دسترسی به اپلیکیشن‌ها را فقط به چیزها یا کسانی که نیاز دارید محدود کنید و با به‌روزرسانی مستمر گوشی و حراست از آن با یک پسورد مستحکم، نکات پایه امنیت موبایل را رعایت کنید.**

توضیحات تکمیلی و فراداده را هم اضافه کنید

وقتی فایل‌ها را روی درایو اوتی‌جی، هارد وایرلس یا گوشی قدیمی‌تان ذخیره می‌کنید، اضافه کردن هرگونه توضیحات تکمیلی و فراداده می‌تواند بسیار مفید باشد. به عنوان مثال، بسیاری از اپلیکیشن‌های مستندسازی و تصویربرداری می‌توانند خروجی‌هایی در فرمت متنی CSV و JSON بدهند که فراداده‌های استخراج‌شده از دستگاه را هم در بر می‌گیرد (اطلاعاتی نظیر موقعیت مکانی، زمان و تاریخ) و هرگونه توضیحی که از سوی کاربر اضافه شده باشد. حتما مطمئن شوید که این فایل‌های متنی فراداده را هم به بک‌آپ‌تان اضافه کرده‌اید.

برای هارد و درایوهای خود رمز عبور بگذارید

برای بسیاری از هاردها و درایوهای وایرلس می‌توانید رمز عبور انتخاب کنید. این کار از طریق اپلیکیشن موبایلی انجام می‌شود که به همراه هارد به کاربر خواهند داد. این نکته را مد نظر داشته باشید که پسورد گذاشتن برای هارد به معنی رمزگذاری (Encryption) آن نیست. اکثر هاردهای وایرلس و اوتی‌جی امکان رمزگذاری کل دیسک با فرمان ارسالی از موبایل را فراهم نمی‌کنند، اما رمزگذاری آنها ممکن است از طریق یک کامپیوتر میسر باشد.

به رمزگذاری فایل‌ها هم فکر کنید

اگر نیاز دارید فایل‌های خود را به صورت امن‌تری ذخیره کنید، می‌توانید نسخه‌های بک‌آپ خود را رمزگذاری کنید. اگرچه شاید نتوانید کل هارد وایرلس یا اوتی‌جی خود را از راه موبایل‌تان رمزگذاری کنید، اما می‌توانید پیش از آن‌که فایل‌ها را به درایو منتقل کنید فرآیند رمزگذاری را به انجام برسانید. اپلیکیشن‌هایی نظیر ZArchiver و RAR امکان رمزگذاری فایل‌ها را روی گوشی‌های اندروید فراهم می‌کنند. به‌هوش باشید که باید پسوردهای رمزگذاری خود را به خاطر داشته باشید. اگر این پسورد را به هر دلیلی از یاد ببرید یا از دست بدهید، هرگز نمی‌توانید به آن فایل‌های رمزگذاری‌شده دسترسی داشته باشید.

این نکته را در ذهن داشته باشید که برخی کشورها ممکن است قوانینی علیه استفاده از امکان رمزگذاری داشته باشند. استفاده از چنین امکانی برای پیش‌گیری از دسترسی مقام‌ها به داده‌های شما، ممکن است به عنوان تلاش برای از بین بردن

شواهد یا مخدوش کردن روند تحقیقات، جرم تلقی شود و قابل پیگرد باشد. این نقشه از سال ۲۰۱۷ ممکن است قدیمی باشد اما اگر درباره قوانین کشورتان پیرامون این موضوع سوالات و ابهاماتی دارید، نقطه شروع مناسبی است.

دو نسخه بک‌آپ در دو مکان مختلف داشته باشید

داشتن فقط یک بک‌آپ همیشه بهترین راه‌حل نیست. به عنوان مثال، اگر ابزاری که بک‌آپ شما روی آن ذخیره شده به هر دلیلی آسیبی ببیند یا کارکردش تصادفا متوقف شود، ممکن است بک‌آپ خود را برای همیشه از دست بدهید. متخصصان فن‌آوری اطلاعات معمولا توصیه می‌کنند که بهتر است دو نسخه بک‌آپ داشته باشید. یعنی در مجموع سه نسخه از یک فایل یا مجموعه فایل خواهید داشت که بهتر است آن‌ها را در مکان‌های مختلف نگه‌داری کنید. به این ترتیب شما از خطرات و تهدیدهایی که ممکن است در انتظار هر یک از نسخه‌ها باشد، می‌کاهید.

آخرین مطلب از این مجموعه را ببینید: «به‌اشتراک‌گذاری فایل‌ها و ارتباط در زمان خاموشی اینترنت»

****

به‌اشتراک‌گذاری فایل‌ها و ارتباطات در زمان خاموشی اینترنت

سرکوب و خاموشی اینترنتی که در کشمیر جاری است، طولانی‌ترین قطعی اینترنت است که در دل یک دموکراسی رخ داده و اثرات فاجعه‌باری بر زندگی مردم این منطقه داشته است. واتس‌اپ هم روی زخم آنها نمک پاشید و در دسامبر ۲۰۱۹ اکانت کشمیری‌ها را به دلیل آن‌که بیش از ۱۲۰ روز غیرفعال بودند، از دسترس خارج کرد. این سیاست واتس‌اپ است.

در هنگام نگارش این مجموعه در ژانویه ۲۰۲۰، دادگاه عالی هند حکم داد که قطعی نامحدود اینترنت در کشمیر «غیرقانونی و سوء استفاده از قدرت» است. در پی صدور این حکم اینترنت پهن‌باند به صورت محدود و اینترنت موبایل به صورت کامل به برخی نقاط کشمیر بازگشت، اما کاربران فقط می‌توانستند به وب‌سایت‌های منتخبی که به «فهرست سفید» اضافه شده‌اند، دسترسی داشته باشند.

هدف از قطع اینترنت این است که امکان به‌اشتراک‌گذاری اطلاعات و برقراری ارتباط برای مردم مسدود شود و آن‌ها چاره‌ای جز روی آوردن به گزینه‌های جایگزین نداشته باشند؛ گزینه‌هایی همچون ارتباط موبایلی و پیامکی که شنودشان آسان‌تر است و امنیت پایین‌تری دارند. پیدا کردن راه‌هایی برای دور زدن محدودیت‌ها در زمان خاموشی سراسری اینترنت آسان نیست. در دوره‌ای که سخت‌ترین محدودیت‌ها در کشمیر اعمال شد و خاموشی سراسری برقرار بود مردم برای ارتباط با عزیزان‌شان به نامه‌های دست‌نوشته و پیک و پست روی آورده بودند.

ما نمی‌توانیم راه‌حل‌هایی قطعی برای دور زدن محدودیت‌ها در زمان قطعی اینترنت ارائه کنیم، اما از خلال گفت‌وگو با کنشگران و کسانی که تجربه زیست در زمان خاموشی را داشته‌اند، دریافته‌ایم که روش‌ها و رویکردهایی برای به‌اشتراک‌گذاری آفلاین و ارتباطات وجود دارند که ممکن است در چنین شرایط بغرنجی به کار بیایند؛ که البته بستگی به شرایط موجود دارند. لطفا در نظر داشته باشید که برای راه‌اندازی برخی از این گزینه‌ها نیاز به دسترسی به اینترنت دارید. یعنی باید اپلیکیشنی را دانلود و آماده بهره‌برداری کنید.

فایل‌ها را از راه بلوتوث، وای‌فای دیرکت یا NFC به اشتراک بگذارید

برای این‌که با گوشی‌تان به دیگر گوشی‌های پیرامون متصل شوید، از راه بلوتوث، وای‌فای دیرکت یا ارتباطات کوتاه‌برد (NFC) نیازی به اینترنت ندارید. روی برخی گوشی‌های قدیمی‌تر اندرویدی برای اشاره به NFC از «اندروید بیم» (Android Beam) استفاده می‌شود. بلوتوث و وای‌فای دیرکت هر دو تکنولوژی‌هایی هستند که می‌توانند دو دستگاه را بدون نیاز به مسیریاب (روتر) یا اکسس‌پوینت دیگری در میانه راه، به هم متصل کنند. وای‌فای دیرکت برد بیش‌تری دارد و انتقال داده‌ها در آن سریع‌تر از بلوتوث است، اما باتری بیش‌تری مصرف می‌کند. ارتباط کوتاه‌برد (ان‌اف‌سی) بردی کم‌تر از ۴ سانتی‌متر دارد و انتقال داده‌ها در آن بسیار کندتر از بلوتوث و وای‌فای دیرکت است، اما سرعت اتصال آن بالاتر است و مصرف باتری بسیار کم‌تری دارد. بنابراین می‌تواند برای انتقال فایل‌های کوچک وقتی هر دو دستگاه در دست‌تان است، گزینه مناسب‌تری باشد.

به احتمال زیاد امکان استفاده از بلوتوث، وای‌فای دیرکت و ان‌اف‌سی روی موبایل شما فراهم است و می‌توانید از میان گزینه‌های به‌اشتراک‌گذاری (Sharing) آن‌ها را پیدا کنید. گذشته از این، اپلیکیشن‌هایی نظیر Files By Google این فن‌آوری‌ها را به امکانات‌شان افزوده‌اند.

نکته مهم: نقطه ضعف اتصال آسانی که با استفاده از این روش‌ها میسر می‌شود این است که این‌گونه ارتباطات امن نیستند. اسکنرهای وای‌فای و بلوتوث می‌توانند به سادگی برای رهگیری موقعیت مکانی شما مورد استفاده قرار گیرند. نفوذگران ممکن است تلاش کنند تا به دستگاه شما متصل شوند، فایل‌های ناخواسته و بدافزار برای‌تان بفرستند یا حتی اگر سیستم‌تان آسیب‌پذیر باشد، کنترل آن را به دست بگیرند. **برای این‌که امن‌تر باشید وقتی از این دستگاه‌ها استفاده نمی‌کنید حتما آن‌ها را خاموش نگه دارید و فقط وقتی به جای امنی می‌رسید آن‌ها را به حالت روشن برگردانید. سطح دسترسی به اپلیکیشن‌ها را فقط به چیزها یا کسانی که نیاز دارید محدود کنید و با به‌روزرسانی مستمر گوشی و حراست از آن با یک پسورد مستحکم، نکات پایه امنیت موبایل را رعایت کنید.**

به‌اشتراک‌گذاری فایل‌ها از طریق درایوهای وایرلس یا شبکه وای‌فای محلی (WLAN)

یک هارد درایو وایرلس یا فلش درایو می‌تواند برای هم‌رسانی فایل‌ها میان اعضای یک تیم یا چندین نفر به صورت هم‌زمان مورد استفاده قرار گیرد. معمولا هاردهای وایرلس به همراه دستورات مشخص یا اپلیکیشن‌هایی عرضه می‌شوند که امکان ارتباط گوشی شما با هارد را فراهم می‌کنند و استفاده از آن‌ها هم نسبتا آسان است. به خاطر داشته باشید که حتما برای افزایش امنیت درایوی که در آن فایل‌ها را ذخیره می‌کنید، رمز عبور بگذارید.

اگر هارد وایرلس در اختیار ندارید، می‌توانید یکی از درایوهای یواس‌بی معمولی را به مسیریاب (روتر) وصل کنید و آن‌گاه فایل‌ها را به اشتراک بگذارید. به عنوان مثال، یک مسیریاب مسافرتی که پورت یواس‌بی دارد را می‌توانید نسبتا ارزان تهیه کنید و نکته این‌که می‌توانید به سادگی آن را به هر جایی که بخواهید حمل کنید. کاربران بدون این‌که به اینترنت دسترسی داشته باشند، می‌توانند به سادگی از طریق یک شبکه محلی به درایو یواس‌بی وصل شوند. برای این‌که بتوانید فایل‌های ذخیره‌شده روی درایو یواس‌بی را روی موبایل‌تان ببینید، باید از اپلیکیشن مدیریت فایلی که به معدن داده‌های شبکه متصل می‌شود استفاده کنید؛ اپلیکیشنی مانند Solid Explorer. آدرس آی‌پی مسیریاب را معمولا می‌توانید در تنظیمات پیشرفته وای‌فای روی موبایل‌تان پیدا کنید.

کاربران می‌توانند به یک درایو یواس‌بی که به یک مسیریاب وایرلس وصل شده، متصل شوند و فایل‌ها را روی شبکه محلی به اشتراک بگذارند.

یکی از گزینه‌های موجود دیگر برای این کار اپلیکیشن PirateBox است. پروژه‌ای که نرم‌افزاری رایگان ارائه کرده که با بهره‌گیری از آن کاربران می‌توانند همان‌طور که در بالا توضیح دادیم، فایل‌ها را به اشتراک بگذارند، با این تفاوت که با «پایرت‌باکس» شما می‌توانید این کار را به صورت ناشناس انجام دهید. امکان چت و پیام‌رسانی هم در این اپلیکیشن ارائه می‌شود. برای راه‌اندازی این اپلیکیشن باید از پیش آن را دانلود و نصب کنید و چند افزونه را هم به آن بیفزایید. توضیحات کامل را می‌توانید در وب‌سایت پایرت‌باکس ببینید.

با استفاده از چت‌های همتابه‌همتا ارتباط برقرار کنید

دو اپلیکیشن پیام‌رسانی نسبتا جدیدی که اخیرا ارائه شده‌اند و از طریق شبکه کنشگران به ما معرفی شده‌اند Briar و Bridgfy هستند که هنوز امتحان‌شان نکرده‌ایم، اما می‌دانیم که گروه‌های دیگری مشغول تست آن‌ها هستند.

«ایران در خاموشی» آنها را آزمایش کرده و اطلاعات بیشتر در جعبه‌ابزارهای ما موجود است:

جعبه‌ابزار اختلال در اینترنت

جعبه‌ابزار قطع اینترنت

جعبه‌ابزار خاموشی کامل

«برایر» یک اپلیکیشن متن‌باز (open-source) است که پیام‌ها را سرتاسری رمزگذاری می‌کند و به سروری مرکزی متکی نیست. برایر به جای ذخیره‌سازی داده‌ها روی یک سرور متمرکز، آن‌ها را روی دستگاه‌های کاربران ذخیره می‌کند. حتی وقتی دسترسی به اینترنت وجود ندارد شما می‌توانید از طریق این اپلیکیشن و مبتنی بر بلوتوث یا وای‌فای (وقتی اینترنت وجود دارد، اپلیکیشن همه دستگاه‌های موجود را از طریق شبکه «تور» همسان می‌کند) به موبایل‌ها و دیگر ابزارهای پیرامون‌تان متصل شوید. برایر امکان ایجاد گروه‌های خصوصی، انجمن‌های عمومی و وبلاگ هم ارائه می‌کند. وقتی به صورت آفلاین از این اپلیکیشن استفاده می‌کنید، برد آن همان حداکثر برد بلوتوث یا وای‌فای است که نزدیک به ۱۰۰ متر است.

از طریق پیامک‌های رمزگذاری‌شده ارتباط برقرار کنید

پیامک‌های متنی روی شبکه‌های موبایل ارسال می‌شوند و برای استفاده از آن‌ها نیازی به دسترسی به اینترنت نیست. احتمال این‌که امکان استفاده از پیامک حتی در زمان خاموشی اینترنت فراهم باشد بالاست. با این همه، اس‌ام‌اس سیستم بسیار ناامنی است. بر خلاف اپلیکیشن‌های مبتنی بر اینترنت نظیر واتس‌اپ یا سیگنال، پیامک‌ها به صورت سرتاسری رمزگذاری نمی‌شوند. این یعنی پیامک‌های متنی و فراداده (metadata) مرتبط با آن‌ها می‌توانند از سوی دولت‌ها یا اپراتورهای موبایل و یا هکرها در میانه راه شنود شوند. امکان جعل شماره‌ها (Spoofing) هم در سیستم پیامک‌رسانی فراهم است، به این معنی که فرستنده می‌تواند وانمود کند دارد از شماره خاصی این پیامک را برای‌تان ارسال می‌کند.

اگر لازم است از اس‌ام‌اس برای برقراری ارتباط استفاده کنید Silence اپلیکیشنی است که اس‌ام‌اس‌ها را سرتاسری رمزگذاری می‌کند. «سایلنس» اپلیکیشنی متن‌باز است و از پروتکل رمزگذاری سیگنال استفاده می‌کند. هنوز خودمان موفق به آزمایش این اپلیکیشن نشده‌ایم، اما گزارش‌هایی از استفاده از آن دریافت کرده‌ایم. برای استفاده از آن، هم فرستنده و هم گیرنده باید اپلیکیشن را دانلود و نصب کرده و کلیدهایشان را با یکدیگر به اشتراک گذاشته باشند. از آن‌جایی که

پیامک‌ها لزوما از مجرای اپراتور موبایل شما رد می‌شوند، حتی با استفاده از سایلنس هم این‌که دارید پیامکی رمزگذاری‌شده می‌فرستید و فراداده آن را هم رمزگذاری کرده‌اید، از طرف شرکت مخابراتی خدمات‌دهنده شما قابل رویت است.

خاموشی موضعی: دور زدن سایت‌های فیلترشده

«خاموشی اینترنت» همیشه به معنی قطع کامل اینترنت نیست. گاهی خاموشی می‌تواند صرفا با مسدود کردن دسترسی به برخی وب‌سایت‌ها یا پلتفرم‌های شبکه‌های اجتماعی همراه باشد. دولت‌ها از طریق خدمات‌دهندگان اینترنت (ISP) می‌توانند وب‌سایت‌ها را بر اساس آدرس آی‌پی، محتوا یا دی‌ان‌اس آن‌ها فیلتر کنند. مطمئن نیستند آیا وب‌سایتی برای شما فیلتر شده یا نه؟ سازمان‌هایی نظیر OONI و «نت‌بلاکس» بر روند فیلترینگ و ایجاد اختلال در اینترنت در سراسر جهان نظارت دارند و گزارش‌های مستمر منتشر می‌کنند.

خوش‌بختانه تا زمانی که دسترسی شما به اینترنت برقرار است، راه‌هایی برای دور زدن محدودیت‌ها و فیلترینگ وجود دارند. همچون رمزگذاری، باید این نکته را در خاطر داشته باشید که تلاش برای دور زدن وب‌سایت‌های فیلترشده هم ممکن است بنا بر قوانین جایی که در آن زندگی می‌کنید، جرم باشد.

وی‌پی‌ان

یک راه برای دور زدن فیلترینگ وب‌سایت‌هایی که بر اساس آدرس آی‌پی یا محتوا فیلتر شده‌اند، استفاده از شبکه خصوصی مجازی، یا همان وی‌پی‌ان است. ProtonVPN و TunnelBear دو نمونه از وی‌پی‌ان‌ها هستند. وقتی از طریق وی‌پی‌ان به اینترنت وصل می‌شوید، ترافیک اینترنت‌تان رمزگذاری شده و از مجرای سرور وی‌پی‌انی که در مکان دیگری (یا حتی کشور دیگری) مستقر است، می‌گذرد. به این ترتیب مقصد نهایی و محتوای ترافیک اینترنت شما از چشم خدمات‌دهنده اینترنت‌تان پنهان می‌ماند.

این نکته را مد نظر داشته باشید که برخی دولت‌ها استفاده از وی‌پی‌ان را ممنوع کرده‌اند و ممکن است تلاش کنند اتصالات وی‌پی‌ان شما را کشف و مسدود کنند. استفاده از وی‌پی‌ان امن و معتبر هم نکته مهمی است و بهتر است از گزینه‌هایی استفاده کنید که داده‌ها و گزارش‌های فعالیت شما را ذخیره نمی‌کنند، چون در آن صورت خدمات‌دهنده اینترنت ممکن است بتواند جزئیات فعالیت‌های شما در اینترنت را ببیند. دقت کنید که خدمات‌دهنده وی‌پی‌ان شما در کدام کشور مستقر است و بسته به موقعیت جغرافیایی آن‌ها، کدام قوانین ممکن است شامل حال شما شود. این نکته را هم در نظر داشته باشید که وی‌پی‌ان‌های مورد تایید دولت‌ها ممکن است در واقع امکان شنود و بازرسی داده‌های شما را برای آن‌ها فراهم کنند.

سرورهای دی‌ان‌اس

سیستم نام‌گذاری دامنه‌ها (DNS) سرورهایی هستند که برای ترجمه نام دامنه‌های اینترنتی یا URLها به آدرس آی‌پی کار می‌کنند. اینترنت، وب‌سایت‌ها را فقط از آدرس آی‌پی آن‌ها می‌شناسد. خدمات‌دهنده اینترنت (ISP) می‌تواند تنظیمات سرورهای دی‌ان‌اسی را که تحت کنترل دارد به‌گونه‌ای تغییر دهد که برخی درخواست‌ها مسدود شوند یا به ازای آن دستورها صفحات نامرتبطی بارگذاری شوند که به شما اعلام می‌کنند دسترسی به وب‌سایتی که می‌خواهید مسدود است. در سال ۲۰۱۴ نخست‌وزیر ترکیه، رجب طیب اردوغان، تلاش کرد تا با بهره‌گیری از همین تکنیک در جریان انتخابات ترکیه دسترسی به توییتر را مسدود کند. این تلاش با واکنش سریع کنشگران که راهنمای گام به گام استفاده از وی‌پی‌ان‌ها و تغییر سرورهای دی‌ان‌اس را منتشر کردند، ناکام ماند.

شما می‌توانید تنظیمات پیش‌فرض سرورهای دی‌ان‌اس (DNS) را روی تنظیمات شبکه یا وای‌فای موبایل خود تغییر دهید. به جای سرورهای دی‌ان‌اس پیش‌فرض، می‌توانید از سرورهای جایگزین از جمله Google Public DNS یا Cloudflare استفاده کنید تا محدودیت‌های دی‌ان‌اس‌محور را دور بزنید. کلاودفلر همچنین اپلیکیشنی به نام 1.1.1.1 دارد که به کاربران اجازه می‌دهد به سادگی به سرورهای دی‌ان‌اس این کمپانی وصل شوند.

شما می‌توانید آدرس‌های دی‌ان‌اس (DNS) را در تنظیمات پیشرفته وای‌فای تغییر دهید. فقط به خاطر داشته باشید که بهتر است پیش از اعمال هر تغییری از تنظیمات پیشین‌تان اسکرین‌شات بگیرید تا در صورت لزوم به آن برگردید.

این‌ها فقط دو راه‌حل موجود برای دور زدن رایج‌ترین تکنیک‌های فیلترینگ‌اند. برای اطلاعات دقیق‌تر و کامل‌تر می‌توانید راهنماهایی را که در این وب‌سایت‌ها ارائه می‌شوند، مطالعه کنید: Internet Society و Access Now و Security-in-a-Box و EFF.