الفبای امنیت
در کنشگری و اعتراضات

درس‌نامه

سعید ملک‌پور

توانا
TAVAANA

الفبای امنیت
در کنشگری و اعتراضات

درس‌نامه

مدرس: سعید ملک‌پور

توانا TAVAANA
آموزشکده آنلاین برای جامعه مدنی ایران
e-collaborative for civic education

www.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

الفبای امنیت در کنشگری و اعتراضات

درس‌نامه

مدرس: سعید ملک‌پور

ناشر: E-Collaborative for Civic Education

پاییز ۱۴۰۳

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

پیش‌گفتار

حفظ حریم خصوصی، امنیت دیجیتال و استفاده امن و صحیح از دستگاه‌های هوشمند، اصول اولیه و ضروری برای تمامی کاربران دنیای دیجیتال است. این موضوع به ویژه برای کنشگران مدنی و سیاسی و شهروندان معترض از اهمیت ویژه‌ای برخوردار است، زیرا نه تنها از آن‌ها محافظت می‌کند، بلکه تأثیرگذاری و کارایی فعالیت‌هایشان را نیز تقویت می‌کند.

با توجه به همین ضرورت، دوره «الفبای امنیت در کنشگری و اعتراضات» با تدریس سعید ملک‌پور - زندانی سیاسی پیشین و برنامه‌نویس کامپیوتر - در تابستان ۱۴۰۳ برای کنشگران و شهروندانی برگزار شد که از فضای مجازی و شبکه‌های اجتماعی برای رساندن صدای اعتراض خود به دیگران استفاده می‌کنند و همچنین در تجمعات اعتراضی، تظاهرات و اعتصاب‌ها شرکت می‌کنند. در این دوره، علاوه بر تأکید بر امنیت دیجیتال، به نحوه حضور امن در تظاهرات و اعتراضات با هدف کاهش خطر دستگیری و شناسایی توسط ماموران نیز پرداخته شد. موضوع امنیت بسیار گسترده است، اما هدف این دوره آموزشی، مرور حداقل‌هایی بود که یک کنشگر یا شهروند مخالف حکومت باید رعایت کند

اکنون درس‌نامه این دوره، شامل متن آموزشی آن، در دسترس شما قرار می‌گیرد. امیدواریم راهکارهای ارائه‌شده در این مجموعه، به شما در پیشبرد اهداف کنشگری و حفظ امنیت بیش‌تر یاری رساند.

درس یک
امنیت سایبری، ۱: تجارب خطرآفرین فعالان سیاسی

در این درس، تجارب خطرآفرین واقعی فعالان سیاسی در استفاده ناامن از دستگاه‌های هوشمند را بررسی می‌کنیم و به ارائه راهکارهایی می‌پردازیم که از اشتباهات منجر به دستگیری جلوگیری می‌کند.

نقش حیاتی امنیت دیجیتال

در دورانی که فعالان سیاسی و مدنی برای فعالیت‌های خود بیش از پیش از ابزارهای دیجیتال و فضای اینترنت استفاده می‌کنند، رعایت نکات ایمنی دیجیتال از اهمیت بیش‌تری برخوردار است. رعایت نکات امنیت دیجیتال نه تنها می‌تواند از فعالان محافظت کند، بلکه اثرگذاری و کارایی فعالیت‌های آن‌ها را نیز تقویت می‌کند.

با استفاده از رعایت هوشمندانه نکات ایمنی دیجیتال، فعالان قادرند هم از خود و هم از دوستان و خانواده خود در مقابل آسیب‌های نیروهای امنیتی و سرکوب محافظت کنند و همچنان باعث تاثیرگذاری چشمگیری در راستای هدف خود باشند.

بهره‌مندی از تجارب فعالان سیاسی

۱. لو دادن هویت به طور ناخواسته در رسانه‌های اجتماعی

در دهه ۹۰، یک گروه از فعالان حقوق بشر که در تهران فعالیت مخفیانه می‌کردند و به

کارهایی از قبیل نوشتن شعار و پخش اعلامیه مشغول بودند، توسط نیروهای اطلاعات سپاه دستگیر شدند. در دوران بازجویی مشخص شد که یکی از اعضای گروه در حین شعارنویسی در تهران عکسی از خود و دوستش گرفته و در صفحه شخصی اینستاگرام خود که خصوصی هم بود، به اشتراک گذاشته است. این گروه با همین اشتباه لو رفته و تمام اعضای گروه دستگیر شده بودند.

این فعال سیاسی نه تنها اشتباه واضح عکس‌گرفتن از خود و دوستانش در یک فعالیت مخفی را انجام داده بود، بلکه آن عکس را در صفحه آنلاین و خصوصی خود نیز به اشتراک گذاشته بود، اشتباه بزرگ دیگر این بود که ایشان تمام درخواست‌های دوستی که در صفحه شخصی‌اش دریافت می‌کرد را بدون این‌که تحقیقی درباره شخص درخواست‌کننده بکند، قبول می‌کرد و نتیجه آن شده بود که یکی از دنبال‌کننده‌های صفحه شخصی او از نیروهای اطلاعات سپاه بوده است. این‌که چرا یک نیروی سپاه به ایشان درخواست دوستی فرستاده نیز این بوده که ایشان با حساب خصوصی خود تعداد زیادی از صفحات دیگر فعالان حقوق بشر را دنبال می‌کرده است.

نیروهای امنیتی و ارتش سایبری گاهی برای خود حساب کاربری غیرواقعی می‌سازند و خود را مخالف نظام معرفی می‌کنند و سعی می‌کنند با ارسال درخواست دوستی به فعالان و دنبال‌کنندهای آن‌ها، اطلاعات جمع‌آوری کنند. بنابراین فراموش نکنید که با رعایت نکات اولیه امنیتی، می‌توانید هم خود و هم دوستان‌تان را از خطر دستگیرشدن و تشکیل پرونده قضایی دور نگه دارید.

اگر می‌خواهید فعالیت‌تان مخفی باقی بماند، هرگز هیچ سندی از آن فعالیت حتی در وسایل شخصی خود نگه ندارید، چیزی که باعث ارتباط‌دادن شما با آن فعالیت باشد، در فضای مجازی به اشتراک نگذارید و نکته مهم‌تر این‌که، اگر صفحه شخصی و خصوصی دارید، با قبول درخواست دوستی افرادی که نمی‌شناسید، صفحه خود را در معرض دید نیروهای امنیتی رژیم قرار ندهید.

شاید به نظر برسد مواردی که گفته شد، بسیار بدیهی باشند و همه به آن عمل می‌کنند، ولی یادمان باشد که بسیاری از فعالان سیاسی و حقوق بشری - که برخی از آن‌ها بسیار افراد شناخته‌شده‌ای هم هستند - با همین اشتباهات ساده، گرفتار دستگاه سرکوب رژیم شده‌اند.

۲. فعالیت در اینترنت بدون استفاده از VPN معتبر

سال ۱۳۸۸ در یکی از اتاق‌های بند ۳۵۰ زندانی جدیدی وارد بند شد و ماجرای دستگیرشدن خود را این‌گونه تعریف کرد که در یک وبلاگ مربوط به انجمن پادشاهی، کامنتی با یک حساب غیرواقعی گذاشته بود و برای نویسنده وبلاگ، آرزوی موفقیت کرده بود. او از این‌که نیروهای امنیتی چطور او را پیدا کرده بودند، شگفت‌زده شده بود! پس از قدری صحبت با ایشان مشخص شد که وبلاگ مورد نظر، در اصل دست نیروهای امنیتی بوده است. این مورد سه حالت بیش‌تر ندارد؛ یکی این‌که ممکن است دارنده و مدیر وبلاگ دستگیر شده و از این طریق کنترل وبلاگ او به دست نیروهای امنیتی افتاده باشد. دوم این‌که وبلاگ مورد نظر به دلیل عدم رعایت نکات ایمنی، توسط ارتش سایبری جمهوری اسلامی هک شده باشد. در حالت سوم که محتمل‌ترین حالت است، وبلاگ با هدف شناسایی هواداران «انجمن پادشاهی ایران»، توسط خود نیروهای امنیتی ساخته شده است. شما زمانی که در یک وبلاگ نظر خود را بگذارید، در صورت عدم استفاده از وی.پی.ان (VPN) امن، آدرس آی.پی (IP Address) شما به همراه کامنت در دیتابیس وبلاگ ثبت می‌شود و صاحب وبلاگ می‌تواند IP شما را ببیند.

در این مورد نیروهای امنیتی با داشتن آی.پی این زندانی سیاسی، ISP یا شرکت ارائه‌کننده اینترنت او را پیدا کرده بودند و با یک استعلام ساده از آن شرکت و دادن آی.پی و زمان دقیق گذاشتن کامنت، به مشخصات و آدرس او رسیده بودند!

در این مورد اگر رعایت نکات اولیه ایمنی صورت می‌گرفت که همان استفاده از وی.پی.ان معتبر برای فعالیت در این فضاها است، حتی با وجود این‌که کنترل این وبلاگ دست نیروهای امنیتی بود، امکان شناسایی این فرد برای آن‌ها وجود نداشت.

این مورد یادآور اهمیت این است که فعالان باید روش‌های ارتباطی امن را برای حفاظت از هویت خود به عنوان اولویت در نظر بگیرند. با توجه به این‌که هیچ گاه نمی‌توان مطمئن بود که پشت یک حساب کاربری آنلاین چه کسی نشسته است، یا این‌که آیا فلان وبسایت نکات امنیتی سایبری را رعایت کرده یا نه، بنابراین اگر قرار است به صورت ناشناس در اینترنت فعالیتی انجام دهیم، بهتر است پیش‌فرض ما همواره این باشد که می‌بایست برای تمام فعالیت‌های خود از وی.پی.ان امن استفاده کنیم تا امکان ردیابی ردپای خود را در اینترنت به هیچ کس ندهیم.

۳. اعتماد به دوستان در فضای مجازی؛ اشتباهی بزرگ در رسانه‌های اجتماعی

در چندین مورد پیش‌آمده، نیروهای امنیتی، به طور مستقیم یا از طریق پرستو - یعنی نیروهای نفوذی حکومت - با نزدیک‌شدن به فعال سیاسی در فضای سایبری اعتماد اشخاص را جلب کرده و از این راه به جمع‌آوری اطلاعات می‌پرداخته و با همین اطلاعات برای اشخاص پرونده قضایی تشکیل داده‌اند. اگر فعالیت سیاسی و مدنی می‌کنید، لازم است به هر کسی که از طریق فضای مجازی یا حتی فضای حقیقی سعی در نزدیک‌شدن به شما دارد، نگاهی مشکوک داشته باشید. اگر قرار است فعالیتی مخفیانه داشته باشید، به هیچ وجه اطلاعات مربوط به این فعالیت را با کسی به اشتراک نگذارید.

به عنوان نمونه مرحوم حبیب اسیود، فعال سیاسی، با اعتمادی که به یک پرستوی ارسالی توسط نیروهای امنیتی، به ترکیه کشانده شد و گرفتار باند آدم‌ربایی نظام شد.

۴. اعتماد صد در صد

روح‌الله زم، فعال سیاسی اعدام‌شده به دست جمهوری اسلامی و شیرین نجفی سال‌ها با هم همکاری داشتند، مرحوم روح‌الله زم به شیرین نجفی اعتماد کامل داشت. بعدها مشخص شد خانم نجفی توسط نیروهای امنیتی دستگیر شده و مجبور به ارتباط با روح‌الله می‌شود و با سناریویی که توسط نیروهای امنیتی ساخته شده بود، روح‌الله به عراق کشانده شده و در آنجا گرفتار شد.

در این مورد روح‌الله به دلیل اعتماد صددرصدی به شیرین نجفی به هیچ یک از عملکرد او مشکوک نشده و گرفتار نقشه شوم نیروهای امنیتی شد. اگر حتی با کسی دوستی و همکاری درازمدت داشتید، باز لازم است که هر از گاهی این پیش‌فرض را داشته باشید که این دوست‌تان ممکن است گرفتار نیروهای امنیتی شده باشد.

۴ نکته امنیتی مهم برای فعالان

با توجه به موارد و تجربه‌هایی که گفته شد، شما به عنوان فعال سیاسی و مدنی، لازم است ۴ نکته امنیتی مهم را در این زمینه رعایت کنید:

۱. سعی کنید کم‌ترین اطلاعات از زندگی خود را در فضای مجازی منتشر کنید. علی‌الخصوص اطلاعاتی که می‌تواند برای شما دردسرساز شود.

۲. اگر می‌خواهید در وب‌سایت، گروه یا کانالی به صورت ناشناس مطلبی بگذارید، مطمئن شوید از وی.پی.ان امنی استفاده کرده‌اید. برای مثال اگر در وبسایت «گرداب» که در مالکیت اطلاعات سپاه است، کامنتی بگذارید و از وی.پی.ان امن استفاده نکرده باشید، اطلاعات سپاه با ردگیری آی.پی شما، به‌راحتی قادر به شناسایی شما خواهد بود.

۳. تقاضای دوستی افراد ناشناس را به هیچ وجه نپذیرید.

۴. اگر فعال سیاسی هستید یا چیزی برای مخفی‌کردن دارید، به هر تماس تلفنی، اینترنتی و تماس از طریق اپ‌ها، مشکوک باشید. حتی اگر دوست صمیمی‌تان با شما تماس گرفت، در نظر بگیرید ممکن است تماس در حضور نیروی امنیتی برقرار شده باشد یا حتی ممکن است آن شخص دوست شما نباشد و با اپلیکیشن‌های هوش مصنوعی صدا یا حتی تصویرش را شبیه‌سازی کرده باشند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- تصاویر و ویدیوهای فعالیت‌های اعتراضی‌مان مثل دیوارنویسی را ...
الف) فقط در کامپیوتر شخصی خود نگه داریم.
ب) فقط در موبایل شخصی خود نگه داریم.
ج) هرگز نباید در دستگاه‌های شخصی خود نگهداری کنیم.
د) می‌توانیم در کامپیوتر خانه که اعضای خانواده از آن استفاده می‌کنند، نگه داریم.

۲- برای فعالیت ناشناس در اینترنت، باید ...
الف) سرویس اینترنت را از یک شرکت معتبر بخریم.
ب) از یک وی.پی.ان امن استفاده کنیم.
ج) از نرم‌افزارهای اصلی (اورجینال) استفاده کنیم.
د) هرگز به کسی پیام ندهیم.

۳- رعایت کدام نکته امنیتی برای فعالان سودمند است؟
الف) انتشار عمومی اطلاعات شخصی زندگی با احتیاط.
ب) انتشار اطلاعات شخصی برای همه کسانی که ما را دنبال می‌کنند.
ج) انتشار اطلاعات شخصی برای کسانی که در لیست مخاطبان‌مان هستند.
د) تا جای ممکن عدم انتشار اطلاعات شخصی و عدم انتشار اطلاعات حساس.

درس دو
امنیت سایبری، ۲: دورزدن امن فیلترینگ

راهکارهای دورزدن فیلترینگ و انتخاب ابزارهای صحیح برای آن

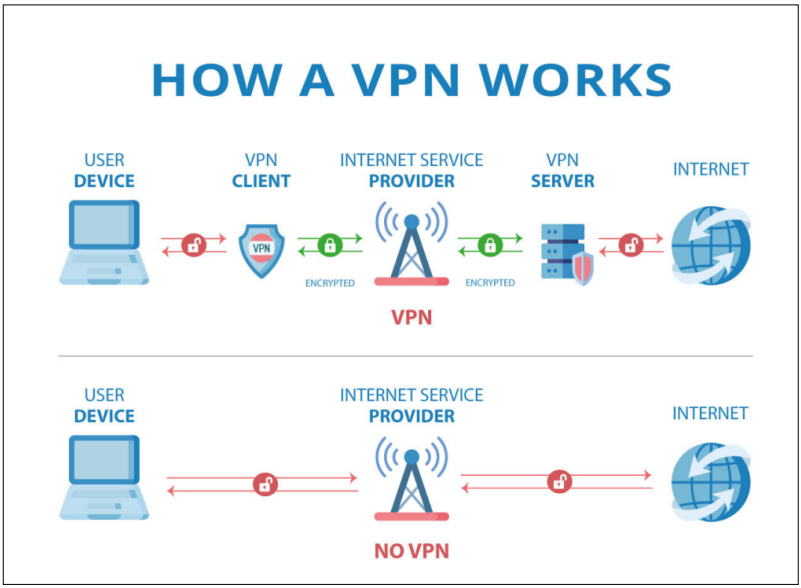
دو راهکار اصلی برای دورزدن فیلترینگ استفاده از وی.پی.ان معتبر و پروکسی‌ها ست در این قسمت به طور مفصل به معرفی هر کدام از آن‌ها می‌پردازیم.

VPN چیست؟

VPN در واقع مخفف «Virtual Private Network» یا «شبکه خصوصی مجازی» است که به کاربر کمک می‌کند تا بدون دسترسی مستقیم به اینترنت، بتوانند به وب‌سایت یا اپلیکیشن‌های آنلاین وصل شود.

هر وی.پی.ان دو بخش دارد، سرور وی.پی.ان (VPN Server) که در اصل سروری است که ما از طریق آن به اینترنت وصل می‌شویم و وی.پی.ان کلاینت (VPN Client) که در واقع ابزار یا اپلیکیشنی است که ما آن را در دستگاه موبایل یا کامپیوتر خود نصب می‌کنیم تا از طریق آن به وی.پی.ان سرور متصل شویم.

همان‌طور که در تصویر بالا می‌بینید، در یک اتصال مستقیم بدون وی.پی.ان، ترافیک اینترنتی، از دستگاه شما به شرکت ارائه‌کننده اینترنت‌تان - مثل همراه اول، ایرانسل و امثال این‌ها - منتقل می‌شود و از طریق اینترنتِ ارائه‌دهنده به اینترنت منتقل می‌شود؛ یعنی



وب‌سایت یا اپلیکیشن‌های مختلف فضای مجازی. در حالت اتصال بدون وی.پی.ان، شرکت ارائه‌کننده اینترنت شما، می‌تواند ببینید که شما به کدام وب‌سایت یا اپلیکیشن متصل شده‌اید. در این حالت آن شرکت می‌تواند ترافیک اینترنت به وب‌سایت یا اپلیکیشن‌های خاصی را مسدود کند؛ که به این کار فیلترینگ گفته می‌شود.

بدون استفاده از وی.پی.ان، این کار برای ارائه‌دهنده اینترنت بسیار سهل و آسان است. همان‌طور که می‌دانیم در ایران، شرکت‌های ارائه‌کننده اینترنت، زیر نظر سیستم اطلاعاتی رژیم فعالیت می‌کنند و اگر سیستم اطلاعاتی اراده کند، می‌تواند از طریق این شرکت‌ها مقصد ترافیک اینترنتی ما را شناسایی و ردگیری کند. یعنی حتی اگر وب‌سایتی فیلتر نباشد، سیستم اطلاعاتی با کمک ارائه‌کنندگان اینترنت می‌تواند ببیند به چه مدت و به کدام وب‌سایت یا اپلیکیشن متصل هستیم و اگر اتصال ما رمزگذاری نشده باشد یا از اپلیکیشن موبایلی استفاده کنیم که از سیستم رمزنگاری استفاده نکرده باشد، سیستم اطلاعاتی حتی به محتوای اطلاعات ردوبدل‌شده توسط ما، دسترسی خواهد داشت.

بنابراین در هیچ حالتی ما نباید اطلاعات حساس یا ارتباطات محرمانه خود را بدون

استفاده از وی.پی.ان مطمئن ردوبدل کنیم. البته در اکثر موارد مانند ارسال ایمیل، از اکثر ارائه‌کنندگان سرویس‌های ایمیلِ معتبر مانند Gmail، Hotmail و Yahoo و برخی اپلیکیشن‌ها مثل Signal یا Telegram secret chat، شرکت ارائه‌دهنده اینترنت تنها متوجه برقراری ارتباط شما با سرور خدمات‌دهنده می‌شود، اما نمی‌تواند محتوای اطلاعات ردوبدل‌شده را ببیند. به این دلیل که این ارتباط در بستر SSL برقرار می‌شود و ارتباط بین شما و سرور در مبدا و مقصد به صورت رمزگذاری‌شده (Encrypted) جابه جا می‌شود و در حالتی که ما از وی.پی.ان استفاده می‌کنیم، اطلاعات توسط VPN Client در دستگاه ما رمزگذاری‌شده و از طریق ISP به VPN Server ارسال می‌شود، این اطلاعات در VPN Server رمزگشایی می‌شود و درخواست ما به وب‌سایت یا اپلیکیشن مورد استفاده ما، ارسال می‌شود.

اطلاعات دریافتی از اینترنت در VPN Server دوباره رمزگذاری می‌شود و توسط ارائه‌کننده اینترنت به VPN Client در دستگاه ما باز می‌گردد. این اطلاعات توسط VPN Client رمزگشایی می‌شود و ما می‌توانیم از آن اطلاعات در جستجوگر اینترنت یا اپلیکیشن موبایل استفاده کنیم.

همان‌طور که مشخص است در این حالت، شرکت ارائه‌کننده اینترنت، تنها چیزی که می‌بیند، ارسال و دریافت یک سری اطلاعات رمزگذاری‌شده بین دستگاه شما و سرور وی.پی.ان است. ارائه‌کننده اینترنت، به دلیل رمزگذاری اطلاعاتی که در سمت server و Client صورت گرفته، به هیچ وجه نمی‌تواند بفهمد که شما به کدام سرور اینترنتی متصل شده‌اید. بنابراین تا زمانی که VPN Server توسط ارائه‌کننده اینترنت شما مسدود یا فیلتر نشده باشد، شما می‌توانید از اینترنت بدون سانسور استفاده کنید.

به دلیل رمزگذاری اطلاعات در وی.پی.ان برای استفاده از وی.پی.ان نیاز به نام کاربری و رمز عبور یا یک کلید دارید. اگر از وی.پی.ان امنی استفاده می‌کنید و اطلاعات محرمانه با آن ردوبدل می‌کنید، بهتر است از کلید یا رمز عبور خود مراقبت کنید و آن را در اختیار دیگران قرار ندهید.

سیستم زیرساخت اینترنت رژیم با بهره‌گیری از تجهیزات و سیستم‌های سانسور که بیش‌تر چینی هستند، می‌تواند تشخیص دهد که ترافیک ردوبدل‌شده یک کاربر می‌تواند ترافیک یک وی.پی.ان باشد و در صورت زیادشدن این ترافیک می‌تواند VPN Server را

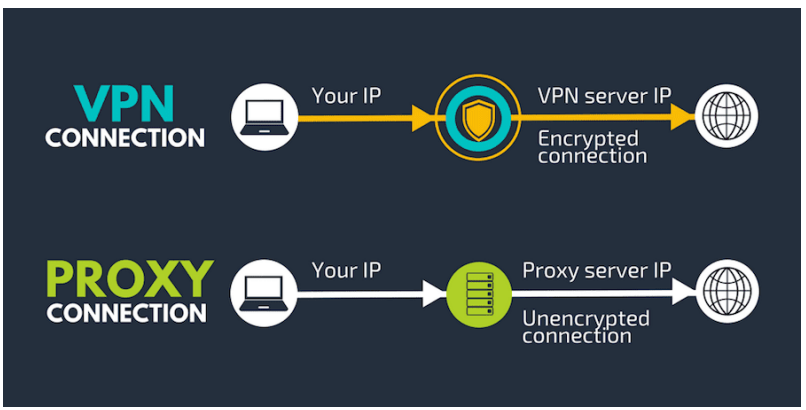
بلاک کند و چیزی که ما می‌بینیم این است که یک وی.پی.ان مدت زمانی کار می‌کند ولی پس از مدتی از کار می‌افتد، دلیلش این است که VPN Server توسط سیستم فیلترینگ شناسایی‌شده و بلاک شده است.

سپاه و سایر سیستم‌های امنیتی جمهوری اسلامی، که کنترل این سیستم فیلترینگ را به عهده دارند، برای سودجویی بیش‌تر و همزمان کنترل بیش‌تر روی مردم، خود اقدام به تولید و پخش و فروش یک سری وی.پی.ان در کشور می‌کنند، با این کار علاوه بر این‌که مقدار زیادی پول به جیب می‌زنند، می‌توانند ترافیک ردوبدل‌شده توسط هر کاربر را ردیابی کنند. بنابراین لازم است دقت کنیم که به هیچ وجه از وی.پی.ان ارائه‌شده توسط رژیم استفاده نکنیم.

برای تهیه یک وی.پی.ان معتبر می‌بایست بسیار وسواس داشته باشیم، همیشه در نظر داشته باشیم، وی.پی.ان‌هایی که در ایران به طور نسبتا آزادانه خرید و فروش می‌شوند، به احتمال خیلی زیاد در دست سیستم اطلاعاتی رژیم هستند.

پروکسی (Proxy) چیست؟

یکی دیگر از راه‌های دورزدن فیلترینگ، استفاده از پروکسی‌ها است اما پروکسی چیست؟ پروکسی‌سرورها بر خلاف وی.پی.ان برای برقراری ارتباط امن ایجاد نشده‌اند. به زبان ساده‌تر پروکسی‌سرور، یک سرور واسط است که از آن برای احراز هویت کاربران و واسطه‌شدن ارتباطات با یک سرویس خاص استفاده می‌شود.



فرض کنید که شما یک پروکسی‌سرور در آلمان دارید و زمانی که به این پروکسی‌سرور متصل شوید، شما را احراز هویت می‌کند و از طرف شما با اینترنت ارتباط می‌گیرد و درخواست‌های شما را دریافت می‌کند و برایتان ارسال می‌کند. پروکسی‌سرور بر خلاف وی.پی.ان رمزگذاری یا رمزگشایی اطلاعات انجام نمی‌دهد. در این تصویر نحوه حرکت اطلاعات در پروکسی را مشاهده می‌کنید.

هر پروکسی‌سرور معمولا برای ارتباط با یک سرور خاص طراحی شده و تنها برای ایجاد یک پل ارتباطی بین شما با یک سیستم یا سروری خاص، مورد استفاده قرار می‌گیرند؛ مانند پروکسی‌های تلگرام و واتس‌اپ. در این سیستم، به دلیل عدم رمزگذاری اطلاعات در پروکسی، شما به نام کاربری یا رمز عبور یا کلید مخصوص نیاز نخواهید داشت.

برخی از اپلیکیشن‌ها در داخل، سیستم رمزگذاری پیشرفته بین خود و سرور دارند که در این موارد استفاده از پروکسی‌سرور مشکل امنیتی خاصی ایجاد نمی‌کند، حتی اگر این پروکسی‌سرور ارائه‌شده توسط سیستم اطلاعاتی باشد، محتوای اطلاعات به دلیل رمزگذاری‌شدن لو نخواهد رفت.

در هر صورت از نظر تئوری، پروکسی‌ها نسبت به وی.پی.ان سرعت بیش‌تری دارند؛ به این دلیل که واحد رمزگذاری و رمزگشایی ندارند و در دستگاه‌های موبایل، مصرف باتری کم‌تری خواهند داشت امل کارایی آن‌ها محدود به یک یا چند سرویس اینترنتی خواهد بود و امنیت آن‌ها نیز نسبت به وی.پی.ان به مراتب کمتر است.

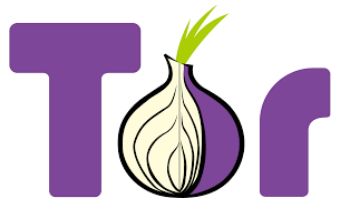
ابزارهای دیگری مانند شبکه تور (Tor) هم برای دورزدن فیلترینگ وجود دارد که در این‌جا به آن می‌پردازیم.

مرورگر تور (Tor browser) چیست؟

مرورگر تور، مرورگری است مانند گوگل‌کروم و فایرفاکس که از تور و چند نرم‌افزار دیگر استفاده می‌کند. مرورگر تور بر پایه فایرفاکس است و تقریبا در همه جا می‌شود آن را به‌راحتی نصب و استفاده کرد.

موارد استفاده از Tor

شبکه تور (Tor Network) شبکه‌ای است که ترافیک وب را ناشناس می‌کند تا یک



وبگردی واقعا خصوصی را ارائه کند. مرورگر Tor آدرس‌آی.پی و فعالیت شما را با هدایت ترافیک وب، از طریق یک سری روترهای مختلف که به عنوان node شناخته می‌شوند، پنهان می‌کند.

اگرچه Tor بیش‌تر به دلیل استفاده‌های غیرقانونی‌اش شناخته شده است، بسیاری از کاربران اینترنت می‌توانند دلایل متفاوت و معتبری برای دسترسی به اینترنت از طریق Tor داشته باشند. این نرم‌افزار آزاد، یک ابزار شبکه‌باز (open network) است که ۳ نوع کار اصلی انجام می‌دهد:

۱- کاهش ردیابی (tracking)

۲- کاهش نظارت دولت‌ها/شرکت‌ها/اشخاص (surveillance)

۳- مقابله با سانسور.

تور در حال حاضر توسط یک شرکت غیرانتفاعی آمریکایی و همچنین داوطلبانی از تمام نقاط جهان اداره می‌شود و هدف اصلیش تحقیق و توسعه ابزارهای امنیت دیجیتال است.

چه کسانی و چرا از Tor استفاده می‌کنند؟

سازمان‌های دولتی: Tor می‌تواند از اطلاعات حساس دولتی محافظت کنند و آن‌ها را به طور ایمن به اشتراک بگذارد. برای مثال سازمان‌های اطلاعاتی درگاه‌های مخصوصی برای ارتباط از طریق دارک‌نت[1] دارند که تنها از طریق Tor قابل دسترسی است.

---

۱. Dark Web یا وب تاریک به شبکه‌ای گفته می‌شود که در دسترس عموم نیست و ردیابی فعالیت‌ها و شناسایی افراد در آن دشوار یا غیرممکن است. در این شبکه اطلاعات جامعی نهفته شده است؛ مانند اطلاعات دستگاه پلیس یا اطلاعات دزدیده شده از کاربران که افراد ناشناس آن‌ها را مدیریت می‌کنند.

شرکت‌ها: شرکت‌هایی که از Tor استفاده می‌کنند می‌توانند از افزایش حریم خصوصی و امنیت داده‌ها بهره‌مند شوند.

سازمان‌های غیرقانونی: گاهی اوقات مجرمان از Tor برای محافظت از فعالیت آنلاین خود استفاده می‌کنند.

افراد معمولی: هر کسی که مایل به حفظ حریم خصوصی آنلاین و امنیت سایبری بهتر است، می‌تواند از مرورگر Tor بهره‌مند شود. روزنامه‌نگاران، فعالان و افرادی که با سانسور مواجه هستند، ممکن است از طریق Tor به تعامل آنلاین بپردازند.

نصب Tor Browser در ویندوز یا مک او.اس

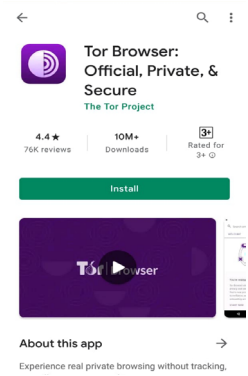
این ابزار را از وب‌سایت اصلی آن دانلود کنید یا یک ایمیل بدون عنوان به آدرس gettor@torproject.org ارسال کنید. اگر لینک دانلود برای ویندوز می‌خواهید در

```
This is an automated email response from GetTor.

You requested Tor Browser for windows.

Step 1: Download Tor Browser

        First, try downloading Tor Browser from either GitLab or GitHub:

        gitlab: https://gitlab.com/thetorproject/torbrowser-10-0-7-windows/raw/master/torbrowser-install-10.0.7_en-US.exe
        Signature file: https://gitlab.com/thetorproject/torbrowser-10-0-7-windows/raw/master/torbrowser-install-10.0.7_en-US.exe.asc

        github: https://github.com/torproject/torbrowser-releases/releases/download/torbrowser-release/torbrowser-install-10.0.7_en-US.exe
        Signature file: https://github.com/torproject/torbrowser-releases/releases/download/torbrowser-release/torbrowser-install-10.0.7_en-US.exe.asc

        If you cannot download Tor Browser from GitLab or GitHub,
        try downloading the file torbrowser-install-10.0.7_en-US.exe
        from the following archives:

        Internet Archive: https://archive.org/details/@gettor

        Google Drive folder: https://drive.google.com/open?id=13CADGTsCwrGsIID09YQbNz2DfRMUoxUU
Step 2: Verify the signature (Optional)

        Verifying the signature ensures that a certain package was generated by its
        developers, and has not been tampered with.  This email provides links to signature
        files that have the same name as the Tor Browser file, but end with ".asc" instead.

        If you run Windows, download Gpg4win and run its installer. In order to verify the
        signature you will need to type a few commands in windows command-line, cmd.exe.

        The Tor Browser team signs Tor Browser releases. Import the Tor Browser Developers
        signing key (0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290):

                gpg --auto-key-locate nodefault,wkd --locate-keys torbrowser@torproject.org

        This should show you something like:

                gpg: key 4E2C6E8793298290: public key "Tor Browser Developers (signing key) <torbrowser@torproject.org>" imported
                gpg: Total number processed: 1
                gpg:               imported: 1
                pub   rsa4096 2014-12-15 [C] [expires: 2020-08-24]
                      EF6E286DDA85EA2A4BA7DE684E2C6E8793298290
                uid           [ unknown] Tor Browser Developers (signing key) <torbrowser@torproject.org>
                sub   rsa4096 2018-05-26 [S] [expires: 2020-09-12]

        After importing the key, you can save it to a file (identifying it by fingerprint here):

                gpg --output ./tor.keyring --export 0xEF6E286DDA85EA2A4BA7DE684E2C6E8793298290
```

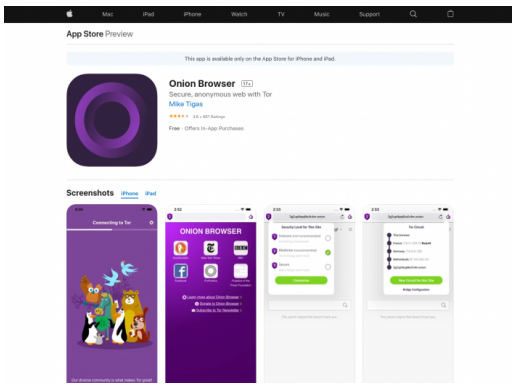
متن نامه کلمه windows و برای مک.او.اس عبارت osx را تایپ کنید. ایمیلی که خواهید گرفت فرمتی به شکل تصویر زیر دارد.

نصب در دستگاه‌های هوشمند

در Android

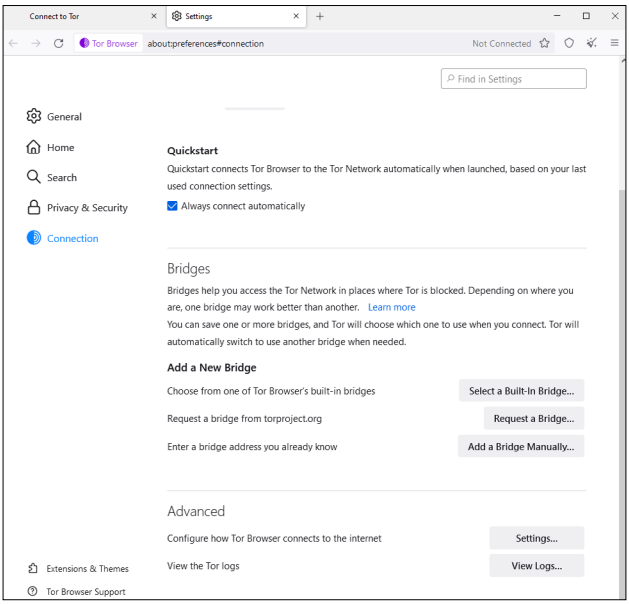


در IOS



اجرای مرورگر تور در دسکتاپ

اگر نتوانستید به شبکه Tor وصل شوید یعنی اتصال شما فیلتر است و باید از یک پل (bridge) استفاده کنید. برای این کار روی گزینه Configure کلیک کنید. در این مرحله سه انتخاب دارید. اگر شبکه تور بلاک باشد، نمی‌توانید مستقیم به آن متصل شوید ولی می‌توانید برای اتصال از پل‌های داخلی استفاده کنید، برای این کار گزینه Select a built-in bridge را انتخاب کنید.

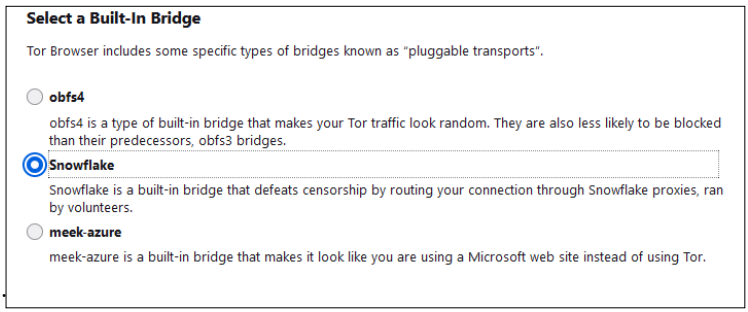


انواع پل‌ها

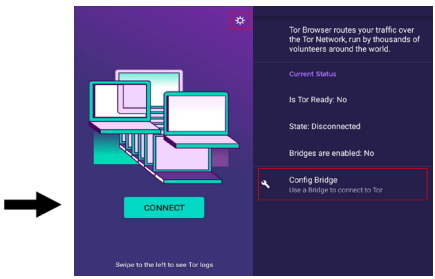
obfs4: نوعی پل داخلی است که ترافیک Tor شما را تصادفی نشان می‌دهد.

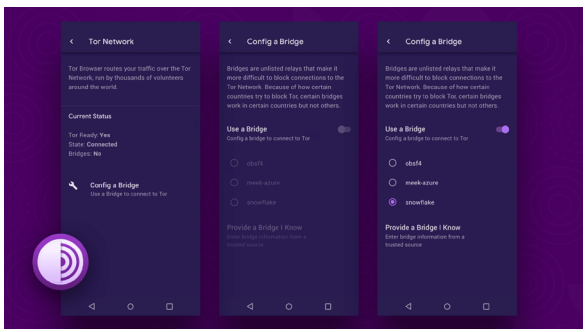
Snowflake: یک پل داخلی است که با مسیریابی اتصال شما از طریق پروکسی‌های Snowflake که توسط داوطلبان اداره می‌شود، کار می‌کند.

meek-azure: یک پل داخلی است که به نظر می‌رسد به جای استفاده از Tor از یک وب‌سایت مایکروسافت استفاده می‌کنید.



برای اجرا در اندروید





پس از این‌که تنظیمات پل را انجام دادید، به صفحه اصلی مرورگر برگردید و روی گزینه Connect کلیک کنید. در صورت عدم موفقیت در اتصال با یک پل، می‌توانید نوع دیگری

را امتحان کنید. در صورت متصل‌شدن می‌توانید از اینترنت بدون فیلتر و تقریبا غیر قابل ردیابی و کنترل استفاده کنید.

۶ نکته مهم برای انتخاب یک VPN یا Proxy معتبر

به هیچ وجه به وی.پی.ان و پروکسی که در ایران به صورت آزادانه خرید و فروش می‌شود، اعتماد نکنید و آن‌ها را نخرید.

هرگز از اپلیکیشن‌های غیر اصلی مثل نسخه‌های فرعی تلگرام و سایر اپ‌ها استفاده نکنید.

در صورتی که خانواده یا دوست صمیمی خارج از ایران دارید، از آن‌ها بخواهید برایتان سرویس‌ها وی.پی.ان معتبر مانند ExpressVPN، NordVPN، UltraVPN، Cyber Ghost و SurfShark خریداری کنند.

هرگز رمز عبور یا کلید وی.پی.ان خود را با کسی به اشتراک نگذارید.

از وی.پی.ان‌های منبع‌باز (Open Source) مانند OpenVPN، OutlineVPN، OrbotVPN، ProtonVPN، WireGuard و Psiphon در صورتی استفاده کنید که ارائه‌دهنده سرورهایشان معتبر باشند.

از طریق صفحات تواناتک یا منابع معتبر می‌توانید راجع به وی.پی.ان سرورهای معتبر اطلاعات بیش‌تری کسب کنید.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام یک از توضیحات زیر به بهترین شکل یک VPN (شبکه خصوصی مجازی) امن را توصیف می‌کند؟

الف) ابزاری که امکان دسترسی امن از راه دور به شبکه را فراهم می‌کند

ب) نوعی نرم‌افزار آنتی‌ویروس.

ج) ابزاری که داده‌های اینترنتی را برای سرعت بیش‌تر، فشرده می‌کند.

د) دستگاه سخت‌افزاری که بدافزار را مسدود می‌کند.

۲- کدام گزاره درباره استفاده از فیلترشکن‌هایی که در ایران آزادانه خرید‌وفروش می‌شوند، درست است؟

الف) اگر فروشنده آن‌ها را می‌شناسیم می‌توانیم استفاده کنیم.

ب) در صورتی که وب‌سایت معتبر و مشتری‌های زیادی دارد می‌توانیم استفاده کنیم

ج) هرگز از آن‌ها استفاده نکنیم.

د) با استفاده از یک ایمیل مستعار، پرداخت را انجام دهیم.

۳- کدام ویژگی برای انتخاب یک وی.پی.ان باید در نظر گرفته شود؟

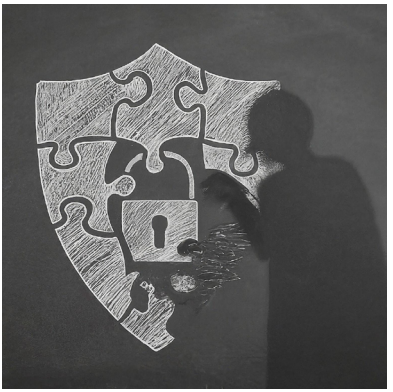
الف) معروف باشد.

ب) خارجی باشد.

ج) دارای رمزنگاری قوی و سیاست حفظ حریم خصوصی شفاف باشد.

و مطمئن شویم اطلاعات ما را لاگ نمی‌کند.

د) هزینه اشتراک آن، ارزان نباشد و گران باشد.



درس سه
امنیت سایبری، ۳: شنود مخابراتی و جاسوس‌افزارها

مقابله با شنود سایبری و جاسوس‌افزارها

وظیفه سیستم اطلاعاتی، بیش‌تر از هر چیز، جمع‌آوری و پردازش اطلاعات به هر طریق است و در این راستا از هر روش ممکن استفاده می‌کند. «شنود» و «جاسوسی از افرادِ هدف»، از کارهای روزمره آن‌ها ست.

شنود مخابراتی؛ مهم‌ترین روش جمع‌آوری اطلاعات

یکی از مهم‌ترین روش‌های کسب اطلاعات نهادهای امنیتی از قدیم، شنود مستقیم مکالمات تلفن و موبایل و اس.ام.اس‌ها بود. اما با ورود دستگاه‌های هوشمند و با توجه به دسترسی کامل نهادهای امنیتی به زیرساخت‌های مخابراتی، می‌توان به‌صراحت گفت که هر فعال سیاسی صاحب دستگاه هوشمند، یک وسیله جاسوسی به همراه خودش دارد، که حتی اگر نهادهای امنیتی موفق نشوند به مکالمات آن‌ها دست پیدا کنند، به‌دست‌آوردن موقعیت مکانی او با یک دستگاه هوشمند روشن در دست‌اش، کار چند ثانیه است.

در همین زمینه، ۱۷ خرداد ۱۳۸۴، روزنامه «هم‌میهن» از ضبط و نگهداری مکالمات

تلفن همراه و پیام کوتاه تا شش ماه توسط وزارت ارتباطات به دستور رییس قوه قضاییه خبر داده بود. بنابراین مهم‌ترین شیوه جمع‌آوری اطلاعات در حال حاضر شنود مخابراتی، و ردیابی موقعیت مکانی شخص دارای دستگاه هوشمند است.

تقریبا غیرممکن است که ما متوجه شنودهایی که از زیر ساخت مخابراتی صورت می‌گیرد، شویم. مکالمات مستقیم تلفن ثابت، موبایل و اس.ام.اس تا چندین ماه در سیستم مخابراتی ذخیره می‌شود و برای سیستم امنیتی در دسترس است.

یکی دیگر از رایج‌ترین انواع شنود، ردیابی مکانی مردم در تجمعات در اعتراضات از طریق بی.تی.اس.های (BTS) محلی است. حدودا از سال ۱۳۹۸، طرح ثبت تلفن‌های همراه با عنوان «جلوگیری از واردات دستگاه‌های تلفن هوشمند قاچاق» در ایران اجرا می‌شود. اما نکته مهم این‌جا ست که سیستم‌های امنیتی پشت این طرح هستند. به زبان ساده می‌توان گفت که ثبت دستگاه‌های هوشمند، یعنی ثبت‌کردن رسمی IMEI دستگاه با یک شماره تلفن در سامانه همتا.

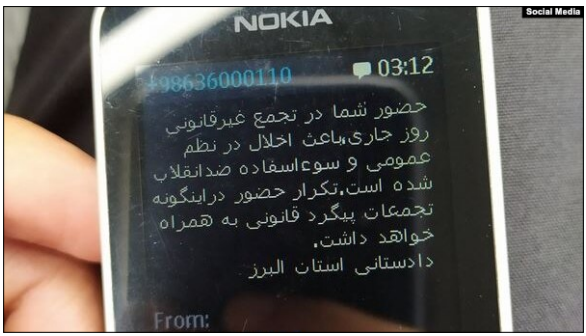
برای درک بهتر این موضوع، باید توضیح دهیم که کد IMEI چیست؟ IMEI برای هر دستگاه هوشمندی به صورت اختصاصی ایجاد می‌شود و در واقع یک کد ۱۵عددی است. از این کد می‌توان به عنوان شناسه دستگاه هم یاد کرد. IMEI در واقع مخفف International Mobile Equipment Identity است و با توجه به اختصاصی‌بودن کد IMEI هر تلفن هوشمندی، بهترین راه برای ردیابی محصول و دسترسی به برخی از اطلاعات است.

پس از روشن‌کردن دستگاه هوشمند برای اولین مرتبه پس از خرید، دستگاه در سیستم مخابرات شناسایی می‌شود و پس از تشخیص دستگاه توسط سیستم، حدود یک ماه فرصت دارید تا برای ثبت دستگاه خود اقدام کنید. اگر در این مدت‌زمان، اصالت دستگاه خود را در سامانه همتا ثبت نکنید، امکان استفاده از سیم‌کارت برایتان نخواهد بود و نمی‌توانید هیچ تماسی بگیرید یا پیامی ارسال کنید.

سیستم امنیتی با ثبت‌نام موبایل، به چه چیزهایی دسترسی دارد؟

با ثبت‌نام هر دستگاه موبایل به نام و شماره شما، تا زمانی که دستگاه تلفن‌تان روشن باشد، حتی اگر سیم‌کارت آن را خارج کنید، دستگاه‌های BTS داخل شهر می‌توانند شما

را ردیابی مکانی کنند. به مفهوم دیگر اگر با موبایل روشن ثبت‌نام‌شده به نام خود، در هر کجای شهر قدم بزنید، توسط سیستم‌های مخابراتی و امنیتی قابل ردیابی هستید. پس فراموش نکنید که اگر می‌خواهید در تظاهرات، تجمع‌ها، تحصن‌ها و هر گونه گردهم‌آیی به صورت ناشناس شرکت کنید، لازم است که موبایل ثبت‌نام‌شده به نام خودتان، در حالت روشن در دست‌تان نباشد، اگر نه سیستم اطلاعاتی که به تمام اطلاعات BTSهای شرکت‌های مخابراتی دسترسی کامل دارد، می‌تواند موقعیت شما را در منطقه متوجه شود



این تصویر، نمونه‌ای از ارسال اخطار به کسانی بود که در یک حرکت اعتراضی در منطقه ای در کرج گرد هم آمده بودند.

۶ روش شنود با نصب نرم‌افزار یا اپ‌های داخلی

۱- شنود از طریق نصب نرم‌افزار (Malware)

سیستم اطلاعاتی با استفاده از نصب نرم‌افزار مالور (Malware)، در دستگاه موبایل، دستگاه تلفن ثابت، لب‌تاپ و تلویزیون هوشمند شما می‌تواند به‌راحتی از شما جاسوسی کند. اگر نکات امنیتی را رعایت نکنید، مهاجم یا نیروی اطلاعاتی با دسترسی فیزیکی یا گاهی از راه دور، قادر به نصب مالور و اسپای‌ور (Spyware) در دستگاه شما هستند.

۲- شنود از طریق خط اینترنت

شنود از طریق آی.اس.پی یا خط اینترنت شما هم از روش‌های مرسوم است که با کمی

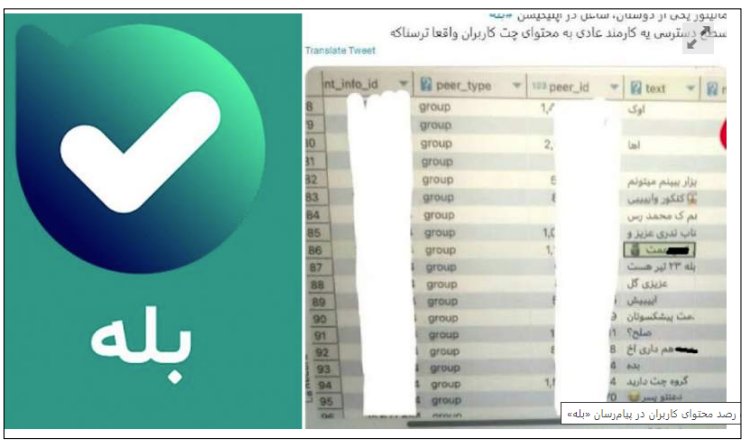
دقت در وبسایت‌هایی که مراجعه می‌کنید و استفاده از وی.پی.ان و مسنجرهای امن می‌توانید از این شنود جلوگیری کنید.

۳- شنود از طریق اپلیکیشن‌های داخلی

یکی دیگر از روش‌های شایع شنود، دستیابی به اطلاعات اپلیکیشن‌های داخلی مثل سرویس‌های اینترنتی تاکسی یا سرویس‌های ارسال غذا، مسنجر یا اپ شبکه‌های داخلی مثل آی‌گپ iGap است. استفاده از این اپلیکیشن‌های ناامن که ممکن است در دستگاه خود نصب داشته باشید، به هیچ عنوان برای فعالان سیاسی توصیه نمی‌شود چراکه راه دسترسی به اطلاعات خود را برای سیستم اطلاعاتی باز می‌کنید.

فراموش نکنید که این اپلیکیشن‌ها مثل iGap که هم اکنون تحت مالکیت سپاه یا متعلق به نیروی اطلاعاتی هستند یا اگر نباشند در صورت درخواست مرجع اطلاعاتی موظف به دادن کلیه اطلاعات شما به آن‌ها هستند.

ماجرای انتشار تصویر اسکرین‌شات یک کارمند عادی اپلیکیشن داخلی «بله» در تیرماه سال ۱۴۰۲ نشان داد که اطلاعات کاربران در این اپلیکیشن‌ها بدون رمزگذاری ذخیره می‌شوند و وقتی یک کارمند عادی «بله» به مکالمات کاربران دسترسی دارد، نشان از این است که سیستم امنیتی هم تمام مکالمات این اپلیکیشن‌ها را تحت رصد خود دارد



رصد محتوای کاربران در پیامرسان «بله»

۴- شنود از طریق وی.پی.ان‌های غیر معتبر

وی پی.ان.هایی که در داخل کشور آزادانه خرید و فروش می‌شوند مستقیم یا غیر مستقیم در دست نهاد امنیتی هستند، و می‌توانند خود راهی برای شنود اطلاعات شما باشند.

۵- شنود سخت‌افزاری

سیستم‌های اطلاعاتی ممکن است در محل کار و زندگی شما، در پریز، در خودرو، داخل کیف، چمدان، اتاق خواب، کانال کولر، سنسور آتش‌سوزی منازل و جاهای زیاد دیگری، سیستم شنود نصب کنند. دقت کنید که یکی از راه‌های نفوذ شنود از طریق پورت یو.اس.بی، «شارژرهای مخصوص برای دزدی اطلاعات» است. همچنین دسترسی فیزیکی حتی کوتاه‌مدت به دستگاه تلفن شما می‌تواند امکانی باشد برای سیستم اطلاعاتی که یا اطلاعات حساس شما را از موبایل‌تان سرقت کنند یا روی دستگاه تلفن‌تان ابزار جاسوسی نصب کنند.

۶- شنود از طریق بلوتوث

پروتکل‌های مورد استفاده در بلوتوث به هیچ عنوان ایمن نیستند. بهتر است همیشه بلوتوث دستگاه خود را غیر فعال نگاه دارید.

آشنایی با ۲ روش نصب دستگاه شنود روی دستگاه تلفن

۱- «روش ریموت» که در اثر غفلت در رعایت نکات ایمنی رخ می‌دهد.

۲- «روش فیزیکی و سخت‌افزاری» که انواع مختلف دارد.
از طریق آشنایان و دوستانی که با آن‌ها نشست و برخاست می‌کنید. یا از طریق موبایل‌قاپ‌ها یا وقتی برای مراجعه به برخی ادارات دولتی که حمل موبایل ممنوع است و باید موبایل‌تان را دم در تحویل دهید، همین می‌تواند فرصتی برای نصب ابزار جاسوسی روی دستگاه شما باشد. این مورد می‌تواند قابل توجه قابل توجه وکلای عزیز باشد. مورد آخر نیز استفاده از شارژرهای عمومی است.

۲۰ راهکار مفید برای مقابله با شنود

۱- هیچ سیستم عامل، نرم‌افزار یا اپ دولتی - از جمله اپ‌های بانکی - در دستگاهی که در آن مکالمات محرمانه انجام می‌دهید، نصب نکنید. به هیچ وجه از اپلیکیشن شبکه‌های اجتماعی داخلی استفاده نکنید.
۲- از وی.پی.ان‌های داخلی استفاده نکنید. استفاده از وی.پی.ان‌هایی که در داخل ایران آزادانه به فروش می‌رسند، اغلب از محصولات سیستم‌های امنیتی نظام هستند و نصب و

استفاده از آن‌ها دعوت از سیستم اطلاعاتی برای دستیابی به اطلاعات و ارتباطات شماست
۳- برای دستگاه خود یک رمز عبور قوی و مناسب انتخاب کنید.
۴- در صورت امکان برای همه حساب‌های خود قابلیت تایید هویت دومرحله‌ای را فعال کنید.
۵- دیواره آتش (Firewall) دستگاه را فعال کنید یا یک فایروال مناسب نصب کنید
۶- آنتی‌ویروس (AntiVirus) و آنتی‌اسپایور (spyware) متناسب با سیستم عامل دستگاه‌تان را نصب کنید و اگر خود دستگاه آن را دارد، فعالش کنید. لازم به ذکر که از آنتی‌ویروسی که مرتب آپدیت نمی‌شود استفاده نکنید به این دلیل که کارایی چندانی نخواهد داشت.
۷- سیستم عامل و اپ‌های دستگاه‌تان را مرتب به‌روز کنید.
۸- از سیستم‌های رمزگذاری برای اطلاعات خود استفاده کنید.
۹- مطمئن شوید تمام ارتباطات شما در محیط رمزگذاری‌شده صورت می‌گیرد.
۱۰- برای محتوای مهم و حساس خود نسخه پشتیبان در یک محل امن تهیه کنید و دقت کنید که نسخه پشتیبان آن هم رمزگذاری شده باشد.
۱۱- تاریخچه جستجو و وب‌گردی خود را پاک کنید.
۱۲- سیستم اتوکامپلیت (Auto complete) گوگل را در دستگاه و نرم‌فزار خود غیر فعال کنید.
۱۳- دستگاه تلفن و لپ تاپ‌تان را حتی برای مدت کوتاه در اختیار کسی قرار ندهید. برای ورود به برخی ارگان‌های دولتی نیاز است دستگاه تلفن‌تان را در ورودی تحویل دهید. در چنین شرایطی بهتر است آن خود را همراه‌تان نبرید.
۱۴- از نسخه‌های غیررسمی اپلیکیشن‌های معروف، مثل نسخه‌های غیررسمی تلگرام، دوری کنید.
۱۵- بلوتوث دستگاه خود را تا جای ممکن در حالت خاموش قرار دهید.
۱۶ - اگر به هر موردی شک کردید، از دستگاه‌های شنودیاب در منزل یا محل کار خود استفاده کنید.
۱۷- ورود افراد غریبه به محل کار، خانه و اتومبیل خود را سخت کنید.
۱۸- هر از گاهی محل کار و زندگی خود را مرتب کنید و جاهایی که امکان شنودگذاری

در آن است را بررسی کنید.
۱۹- فقط و فقط از شارژر خودتان برای شارژ موبایل و سایر دستگاه‌تان استفاده کنید.
۲۰- در استوری و پست‌های شبکه‌های اجتماعی راجع به موقعیت مکانی فعلی خود چیزی به اشتراک نگذارید. برای مثال اگر در پست اینستاگرام راجع به سفر یک‌هفتگی خود با دوستان به شمال عکس می‌گذارید، یعنی به سیستم اطلاعاتی اطلاع داده‌اید که خانه یا محل کارتان خالی ست و مناسب برای عملیات نصب شنود.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- استفاده از اپلیکیشن‌های پیام‌رسان داخلی...

الف) مشکلی ندارد، اگر بدانیم با چه کسی صحبت می‌کنیم.

ب) مشکلی ندارد، اگر فقط برای صحبت‌های روزمره باشد.

ج) درست نیست، مگر این‌که تایید هویت دومرحله‌ای را فعال کنیم.

د) اصلا درست نیست و هرگز نباید استفاده کرد.

۲- وی.پی.ان‌های داخلی می‌توانند ابزار شنود کاربران باشند.

الف) کاملا درست نیست.

ب) کاملا درست است.

ج) درست است، اگر معروف نباشند.

د) درست است، اگر ارزان باشند.

۳- اگر می‌خواهید به صورت ناشناس در یک تظاهرات یا تجمع اعتراضی شرکت کنید، می‌توانید موبایلی که به نام خودتان ثبت شده است را همراه داشته باشید اگر...

الف) بلوتوث آن خاموش باشد.

ب) وای‌فای آن خاموش باشد.

ج) اصلا روشن نباشد.

د) موقعیت مکانی (Location) آن خاموش باشد.

درس چهار
امنیت سایبری، ۴: رمزگذاری و ارتباط امن

ایجاد ارتباط امن با ابزارهای مناسب و آشنایی با ابزارهای رمزگذاری

با توجه به افزایش روزافزون حملات سایبری و جاسوسی توسط هکرها و سیستم‌های امنیتی حکومت، حفاظت از اطلاعات برای فعالان سیاسی و مدنی به یک نقش حیاتی تبدیل شده است. در این راستا، استفاده از ابزارهای رمزگذاری به عنوان یک راهکار اساسی برای مقابله با چالش‌های امنیتی مطرح می‌شود.

با توجه به تحولات سریع در دنیای دیجیتال، افرادی که در زمینه‌های سیاسی و مدنی فعالیت می‌کنند، نیازمند استفاده از ابزارهای امنیتی مدرن هستند. ایجاد ارتباطات امن و آشنایی با ابزارهای رمزگذاری نیز می‌تواند مخاطرات مرتبط با حفظ امنیت اطلاعات آنان را به حداقل برساند. این تدابیر نه تنها به فعالان اجازه می‌دهد تا فعالیت‌های خود را بدون هرگونه نگرانی از امنیت اطلاعات انجام دهند، بلکه به حفظ حقوق حریم شخصی آنان نیز کمک می‌کند.

۲ ابزار رمزگذاری و ارتباط امن

۱- شبکه‌های افتراقی (VPN)

استفاده از وی.پی.ان به فعالان سیاسی و مدنی این امکان را می‌دهد که ارتباطات خود را از

طریق یک شبکه امن و رمزگذاری‌شده انجام دهند.

یک وی.پی.ان امن به افراد اجازه می‌دهد تا هویت و مکان فیزیکی خود را مخفی نگه دارند. در این خصوص در جلسه قبلی به تفصیل صحبت کردیم.

۲. اپلیکیشن‌ها و پلتفرم‌های پیام‌رسان با قابلیت رمزگذاری اطلاعات

استفاده از اپلیکیشن‌ها و پلتفرم‌های پیام‌رسان با قابلیت رمزگذاری، امکان ارسال اطلاعات به صورت امن و بدون نگرانی از نفوذ فرد سوم را فراهم می‌کند. در این اپلیکیشن‌ها، متن یا اطلاعات قبل از ارسال به گیرنده رمزگذاری می‌شوند و در صورت شنود اطلاعات در مسیر ارتباطی، هکر یا جاسوس نمی‌تواند به محتوای آن دست یابد.

۲ ابزار امن برای مواقع برقراری اینترنت و داشتن VPN مناسب

۱- اپلیکیشن سیگنال

سیگنال (Signal) یک برنامه پیام‌رسان بسیار معتبر است که به دلیل تاکید ارائه‌کنندگان آن بر حریم خصوصی و امنیت شناخته می‌شود. در ادامه، ۹ ویژگی و جنبه کلیدی برنامه را بررسی می‌کنیم.

۱ - رمزنگاری انتهابه‌انتها (end to end)

سیگنال از سیستم رمزنگاری end to end برای تمامی ارتباطات استفاده می‌کند، که به معنای این است که تنها گیرنده مقصد قادر به رمزگشایی و خواندن پیام‌ها است. این به این معنا ست که حتی سرورهای سیگنال هم قادر به دسترسی به محتوای پیام‌ها نیستند.

۲- منبع‌باز

کد منبع سیگنال باز است و برای بازبینی عمومی در دسترس است. این شفافیت به افراد حقوقی و جامعه، اجازه تجزیه و تحلیل کد را می‌دهد و به افزایش اعتماد و اعتبار کمک می‌کند.

۳- سازگاری با پلتفرم‌ها و سیستم‌های عامل مختلف

سیگنال برای پلتفرم‌های مختلف شامل iOS، Android و سیستم‌های عامل دسکتاپ در دسترس است. این سازگاری چند پلتفرم به کاربران این امکان را می‌دهد که به صورت امن از دستگاه‌های مختلف با یکدیگر ارتباط برقرار کنند.

۴- تماس‌های صوتی و تصویری امن

علاوه بر پیام‌های متنی، سیگنال از تماس‌های صوتی و تصویری امن نیز پشتیبانی می‌کند. اصول رمزنگاری انتهابه‌انتها به این نوع از ارتباطات نیز اعمال می‌شود که حریم خصوصی مکالمات را تضمین می‌کند.

۵- پیام‌های حذف‌شونده خودکار

سیگنال امکان ارسال پیام‌های حذف‌شونده را فراهم کرده است که به کاربران این امکان را می‌دهد که طول عمر پیام‌ها را تنظیم کنند. پس از گذشت زمان مشخص، پیام‌ها به طور خودکار از هر دو دستگاه حذف می‌شوند.

۶- امنیت صفحه

سیگنال ویژگی‌های امنیتی را پیاده‌سازی کرده است تا حریم خصوصی را بهبود دهد، از جمله جلوگیری از گرفتن اسکرین‌شات در داخل برنامه. این یک لایه اضافی از حفاظت در برابر ضبط غیرمجاز اطلاعات حساس ارائه می‌کند.

۷- ثبت‌نام بدون نیاز به اطلاعات شخصی

سیگنال به کاربران امکان ثبت‌نام بدون نیاز به شماره تلفن را می‌دهد. این ویژگی حفظ ناشناسی و حریم خصوصی را برای کسانی که تمایل به افشای شماره تلفن خود ندارند، افزایش می‌دهد. از طرف دیگر برای کاربران ایرانی که لازم است برای ثبت‌نام از شماره تلفن موبایل در بیش‌تر اپلیکیشن‌ها استفاده کنند، تهدید ریکاوری اکانت با استفاده از شماره تلفن توسط سیستم‌های امنیتی از بین می‌رود.

۸- گروه‌های چت امن

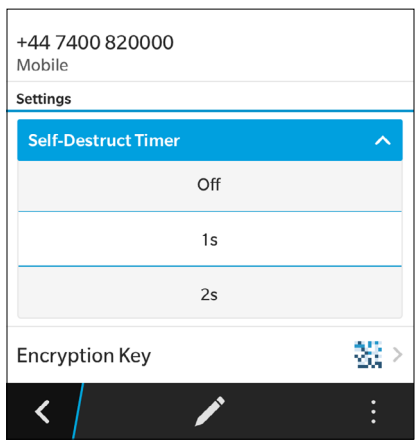
کاربران می‌توانند گروه‌های چت امن در سیگنال ایجاد کنند. اصول رمزنگاری انتهابه‌انتها در مکالمات گروهی نیز اعمال می‌شود که محتوای چت از دسترس طرف سوم‌ها محافظت می‌شود.

۹- ویژگی‌های امنیتی پیشرفته

سیگنال به طور مداوم ویژگی‌ها و پروتکل‌های امنیتی خود را به‌روزرسانی می‌کند تا با تهدیدات نوظهور مقابله کند.

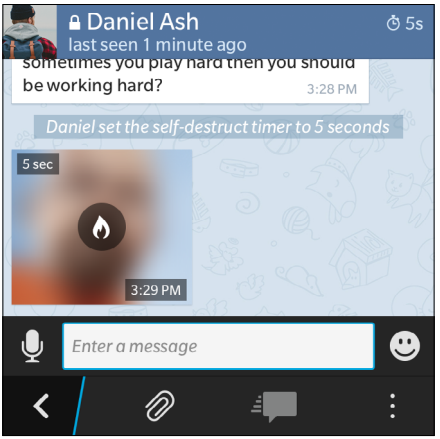
۲ - سکرت‌چت تلگرام

سکرت‌چت (Secret Chat) یک ویژگی امنیتی در اپلیکیشن تلگرام است که امکان برقراری چت‌های رمزگذاری‌شده با ویژگی‌های خاص برای حفظ بیش‌تر حریم خصوصی را فراهم می‌کند. یکی از ویژگی‌های مهم آن امکان تعیین زمان نمایش برای پیام و عکس‌های ارسالی است.



اگر طول عمر یک عکس یک دقیقه یا کمتر تنظیم شود، تلگرام با تارکردن پیش‌نمایش تصاویر و نمایش آن‌ها در صورت لمس صفحه، به ما کمک می‌کند که در مکان‌های عمومی

کسی نتواند مخفیانه از پشت سر تصاویر چت را دید بزند.



به محض این‌که با زدن روی شعله عکس به نمایش در خواهد آمد و یک شمارش معکوس خواهیم دید که پس از آن تصویر حذف می‌شود.

البته ابزارهای امن برای ارتباط تنها به سیگنال و سکرت‌چت تلگرام محدود نیستند. تمامی مسنجرهایی که رمزگذاری end-to-end را پشتیبانی می‌کنند در صورت استفاده صحیح، ابزار امن محسوب می‌شوند.

Bridgefy؛ ابزاری امن برای زمان قطعی اینترنت

Bridgefy یک اپلیکیشن پیام‌رسان آفلاین است که امکان برقراری ارتباط در شرایطی که اینترنت قطع شده و محدودیت‌های شدید را به کاربران می‌دهد. کاربران می‌توانند با روشن‌کردن بلوتوث موبایل خود، در شرایطی که امکان استفاده از اینترنت وجود ندارد، با دوستان و کسانی که در نزدیکی آن‌ها حضور دارند، ارتباط برقرار کنند. بنابراین این یکی از بهترین ابزارها برای افراد شرکت‌کنندگان در تظاهرات‌ها است.

در شرایط خاصی مانند آبان ۱۳۹۸، که اینترنت به طور کلی قطع شد و امکان برقراری تماس از طریق شبکه اینترنت وجود نداشت، اپلیکیشن Bridgefy می‌توانست

به عنوان یک گزینه امن و کارآمد برای برقراری ارتباط در این شرایط بحرانی مطرح شود. این اپلیکیشن برای سیستم‌عامل‌های اندروید و آی.او.اس - در آیفون و آیپد - در دسترس است و به ۴ حالت مشخص کار می‌کند:

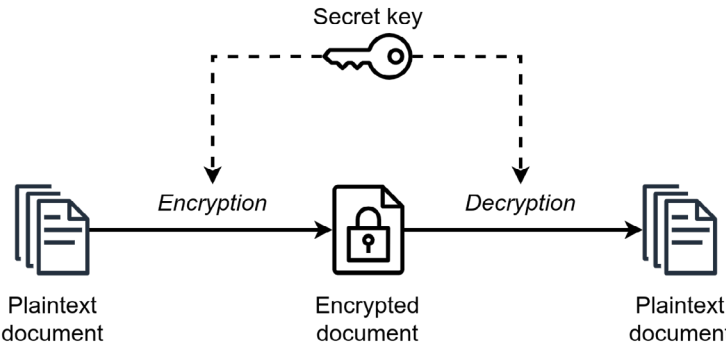
۱. **فردبه‌فرد:** در این حالت بلوتوث دستگاه خود را روشن کنید و با دوستان‌تان که در محدوده ۱۰۰متری شما هستند، به صورت خصوصی صحبت کنید.
۲. **شبکه‌ای:** برای ارتباط با افرادی که خارج از محدوده ۱۰۰متری قرار دارند، در حالت شبکه‌ای، شما می‌بایستی از امکان دیگر کاربران این پیام‌رسان که در «میانه» مسیر قرار دارند، استفاده کنید. به عنوان مثال اگر فرد شماره یک بخواهد با فرد شماره ۳ در فاصله ۱۵۰ متری ارتباط برقرار کند، در میان این دو نفر، یک فرد شماره ۲ لازم است که فاصله‌اش از هر دو این‌ها کمتر از ۱۰۰ متر باشد و از این پیام‌رسان هم استفاده کند. همین مورد می‌تواند برای تعداد نامحدودی از افراد و به صورت زنجیره‌ای پیش رود. البته نگران نباشید، چرا که پیام‌های ردوبدل‌شده شما و فرد مورد نظرتان کاملا امن هستند و افراد «میانی» امکان دسترسی و خواندن آن‌ها را ندارند. در یک جمعیت زیاد هر چه تعداد استفاده‌کنندگان این اپلیکیشن بیش‌تر باشد، شعاع شبکه و سرعت انتقال اطلاعات بیش‌تر خواهد شد.
۳. **پخش عمومی**: شما با واردشدن به بخش Broadcast می‌توانید به طور هم‌زمان پیام‌های خود را برای تمامی کاربران Bridgefy در اطراف خود بفرستید، حتی اگر آن‌ها در لیست مخاطبین شما نباشند!
۴. **حالت آنلاین:** شما می‌توانید از طریق اتصال به اینترنت با دوستان خود به صورت آنلاین در هر کجای دنیا که هستند، صحبت کنید.

رمزگذاری فایل‌ها، روشی برای امنیت دیجیتال

یکی دیگر از راه‌های محافظت از اطلاعات حساس، استفاده از ابزارهای رمزگذاری برای فایل‌ها و اسناد دیجیتالی است تا به این ترتیب از دسترسی غیرمجاز به این اطلاعات جلوگیری شود. این مسئله برای فعالانی که اسناد مهم و حساس خود را در دستگاه‌های کامپیوتر یا موبایل خود نگهداری می‌کنند، به عنوان یک ضرورت الزامی مطرح می‌شود. هیچ گاه مدارک و فایل‌های مهم را بدون رمزگذاری در دستگاه خود ذخیره نکنید. ابزارهای

مختلفی برای رمزگذاری اطلاعات وجود دارند که عمده آن‌ها در ۲ رده تقسیم‌بندی می‌شوند:

۱- ابزارهای رمزنگاری متقارن



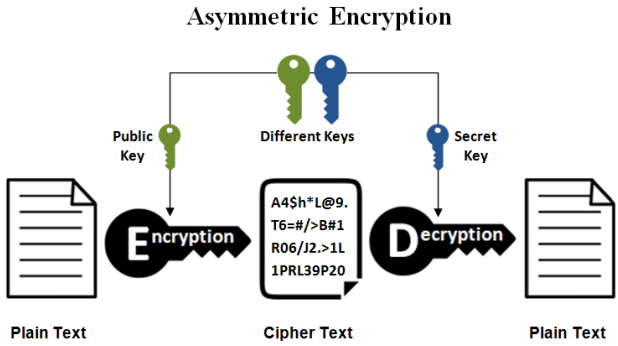
برای درک الگوریتم‌های رمزنگاری، مثال‌های ملموس بهترین ابزارها هستند. بنابراین فرض کنید فرستنده، پیام محرمانه خود را داخل یک جعبه می‌گذارد و در آن را با قفلی مخصوص می‌بندد که کلیدش را در اختیار دارد. گیرنده، یک نمونه مشابه همان کلید را در اختیار دارد که قبلا به هر روشی - مثلا حضوری - از فرستنده گرفته است. او با استفاده از کلید، جعبه را باز می‌کند و پیام را می‌خواند.

این روش رمزگذاری برای فایل‌های بزرگ و مدارک موجود در کامپیوتر شخصی و تلفن همراه، گزینه مناسبی است زیرا تنها شما هستید که می‌بایست پسورد را به خاطر بسپارید.

۲- ابزارهای رمزنگاری نامتقارن

الگوریتم رمزنگاری نامتقارن از یک جفت کلید استفاده می‌کند که یکی از آن‌ها کلید مخفی (secret key) است و یکی از آن‌ها عمومی است. این دو کلید از لحاظ ریاضی با یکدیگر در ارتباط هستند.

فرض کنید یک جعبه دو کلید دارد، با یک کلید می‌شود این جعبه را قفل کرد ولی نمی‌توانید جعبه را با همان کلید باز کنید! کلیدی که با آن جعبه را قفل می‌کنید در این



روش، کلید عمومی است و در دسترس همگان است ولی برای بازکردن این جعبه نیاز به کلید دوم است که به آن secret key یا کلید مخفی می‌گوییم و تنها گیرنده، آن را در اختیار دارد. فرستنده، ابتدا از گیرنده می‌خواهد که کلید عمومی خود را برای او بفرستد سپس فرستنده پیام را در جعبه‌ای می‌گذارد و با همان کلید عمومی آن را قفل می‌کند. پس از ارسال پیام، در جعبه قفل‌شده، فقط گیرنده امکان بازکردن پیام را خواهد داشت، چون کلید مخصوص یا همان کلید مخفی را در اختیار دارد. حتی خود فرستنده هم پس از قفل‌کردن جعبه، دیگر امکان بازکردن آن را نخواهد داشت.

این نوع رمزگذاری برای ارسال اطلاعات بهترین انتخاب است، زیرا لازم نیست کلید مخفی را برای فرستنده ارسال کنیم. هکرها حتی با داشتن کلید عمومی هم قادر به بازکردن اطلاعات نخواهند بود. وب‌سایت‌ها و اپلیکیشن‌ها بیش‌تر از روش نامتقارن برای رمزگذاری اطلاعات استفاده می‌کنند.

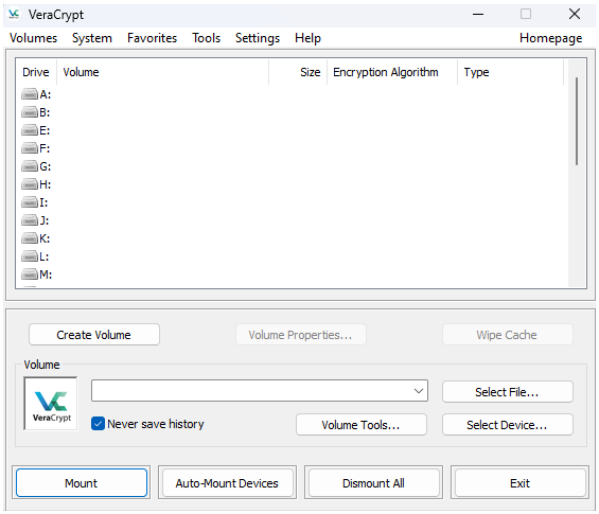
برای مثال مرورگر شما هنگام نصب، یک زوج کلید در دستگاه شما ساخته که منحصر به دستگاه شماست، هرگاه می‌خواهید به وب‌سایتی با قابلیت SSL مانند GMail متصل شوید، مرورگر شما کلید عمومی وب‌سایت Gmail را گرفته و کلید عمومی مرورگر را برای سرور gmail ارسال می‌کند، تمامی اطلاعات ارسالی از طرف شما به سرور Gmail با کلید عمومی Gmail رمزگذاری می‌شود و تمام اطلاعات شما در سرور Gmail با کلید عمومی مرورگر شما رمزگذاری می‌شود. لذا اگر اطلاعات ارسالی بین مرورگر و gmail شنود شود، باز هکر نمی‌تواند به آن اطلاعات دسترسی داشته باشد. زیرا کلید خصوصی

شما یا سرور gmail را در اختیار ندارد.

VeraCrypt؛ نرم‌افزاری برای رمزگذاری فایل یا دایرکتوری

VeraCrypt ابزاری است که ولوم‌های رمزنگاری‌شده ایجاد می‌کند تا بتوانید محتوای خود را به صورت ایمن در آن‌ها ذخیره کنید. همچنین به شما اجازه رمزنگاری تمامی درایوها و پارتیشن‌های سیستم را نیز می‌دهد.

شما می‌توانید از وبسایت رسمی این نرم‌افزار به آدرس آن را دانلود کنید. این نرم افزار برای تمامی سیستم عامل‌های شناخته‌شده کامپیوترهای شخصی قابل اجراست.



نحوه ساخت والیوم توسط VeraCrypt

برای ساخت یک ولوم توسط VeraCrypt، گزینه Create Volume را بزنید. با این کار سه گزینه برای شما نمایش داده می‌شود:

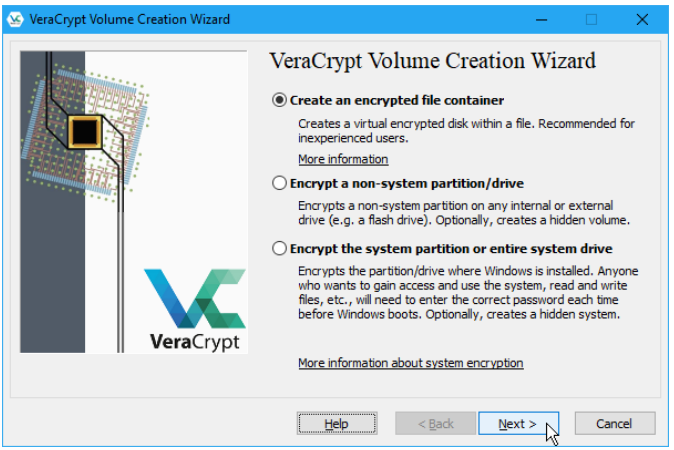
۱. گزینه Create an encrypted file container یک دیسک مجازی برای نگه‌داری فایل‌ها ایجاد می‌کند.

۲. گزینه Encrypt a non-system partition/drive یک درایو غیر سیستمی

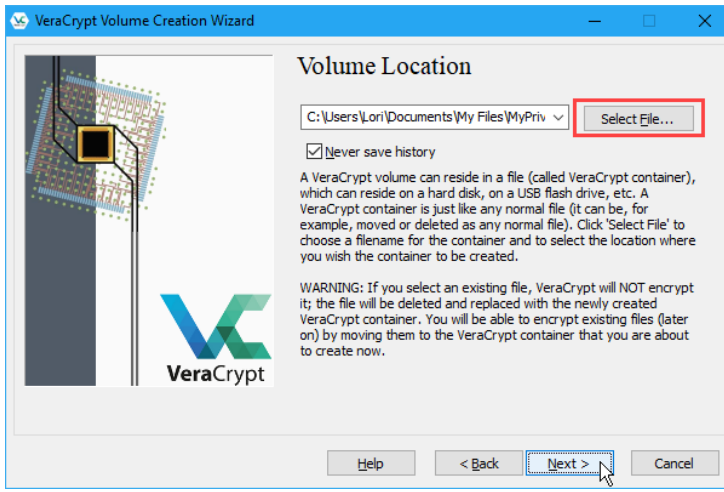
را رمزنگاری می‌کند - یعنی درایو یا پارتیشنی که سیستم عامل در آن قرار نداشته باشد. همچنین از این گزینه می‌توانید برای ساخت یک ولوم مخفی نیز استفاده کنید.

۳. گزینه Encrypt the system partition or entire system drive درایوی که ویندوز در آن نصب شده باشد را رمزنگاری می‌کند. امکان ساخت یک درایو سیستم مخفی نیز وجود دارد. برای مثال ما می‌خواهیم یک ولوم رمزنگاری‌شده برای ذخیره‌سازی فایل‌های شخصی ایجاد کنیم، در نتیجه گزینه مد نظر ما، گزینه Create an encrypted file container است.

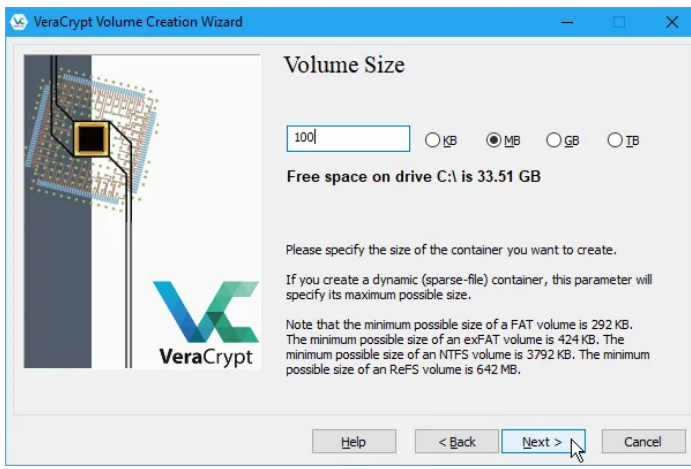
۴. پس از انتخاب گزینه مورد نظر، روی Next کلیک کنید.



در صفحه Volume Location روی گزینه Select File بزنید و از پنجره‌ای که باز می‌شود، برای انتخاب محل قرارگیری فایل ولوم VeraCrypt استفاده کنید.

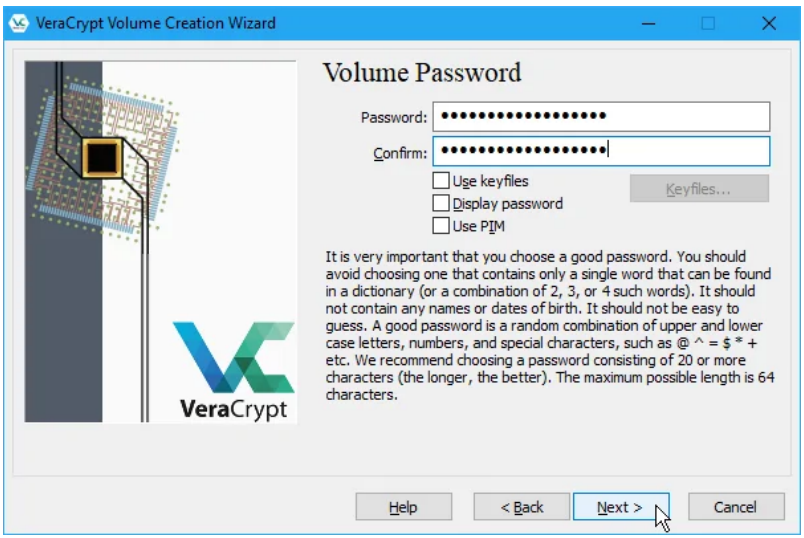


سایز Volume متناسب با حجم اطلاعات خود را وارد کنید و روی Next کلیک کنید.



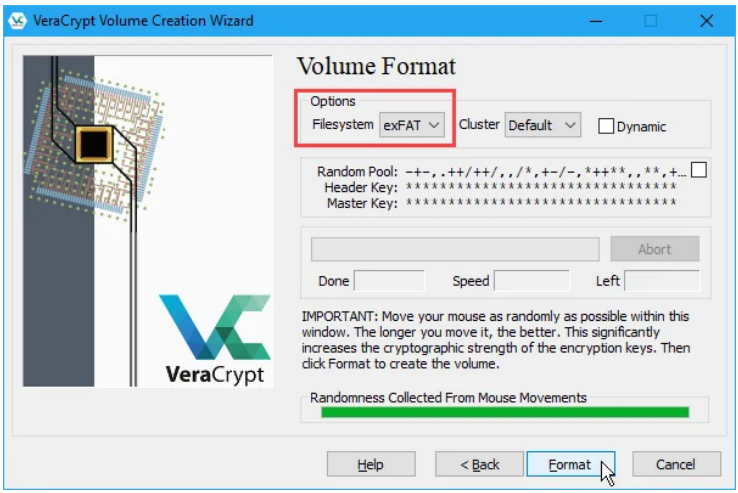
یک رمز عبور مناسب برای Volume خود انتخاب کنید. پسورد انتخابی می‌بایست ۵ ویژگی مشخص داشته باشد:

۱. رمز عبور نباید در لغت‌نامه موجود و قابل پیداکردن باشد.
۲. باید شامل اعداد و کاراکترهای خاصی نظیر @، ! و امثال آن باشد.
۳. رمز عبور باید مجموعه‌ای از حروف بزرگ و کوچک را در خود داشته باشد.
۴. باید حداقل شامل ۱۰ کاراکتر شود.
۵. در نهایت، رمز عبور نباید چیزی باشد که به‌سادگی بر اساس اطلاعات شخصی نظیر تاریخ تولد، کد پستی یا شماره تماس فرد، قابل حدس‌زدن باشد.



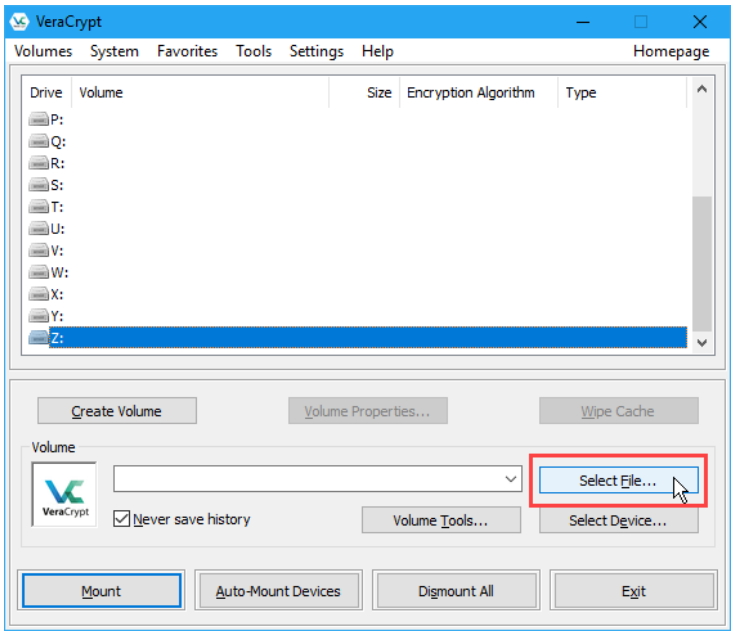
پس از انتخاب رمز عبور، در صفحه Volume Format، فایل‌سیستم مورد نظر خود را انتخاب کنید. اگر علاوه بر ویندوز، قصد استفاده از این ولوم در سیستم لینوکس یا مک را دارید، از FAT یا exFAT استفاده کنید. سپس گزینه Cluster را روی Default قرار دهید و از فعال‌کردن گزینه Dynamic خودداری کنید. پس از همه این اقدامات، ماوس خود را به صورت تصادفی در صفحه Volume Format حرکت دهید تا نوار زیر گزینه

Randomness Collected From Mouse Movements به رنگ سبز در بیاید. به این ترتیب VeraCrypt، رمزنگاری ولوم شما را به صورت شانسی از روی حرکت ماوس‌تان ایجاد خواهد کرد. هر چه ماوس خود را بیش‌تر تکان دهید، رمزنگاری ولوم هم قوی‌تر خواهد بود. در نهایت روی گزینه Format کلیک کنید و اگر پیغام User Account Control نمایش داده شد، گزینه Yes را انتخاب کنید.

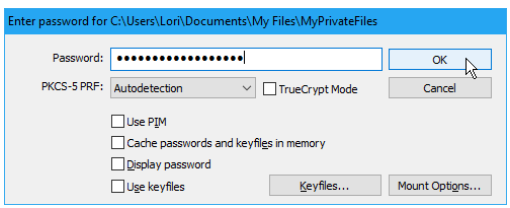


استفاده از Volume ساخته‌شده

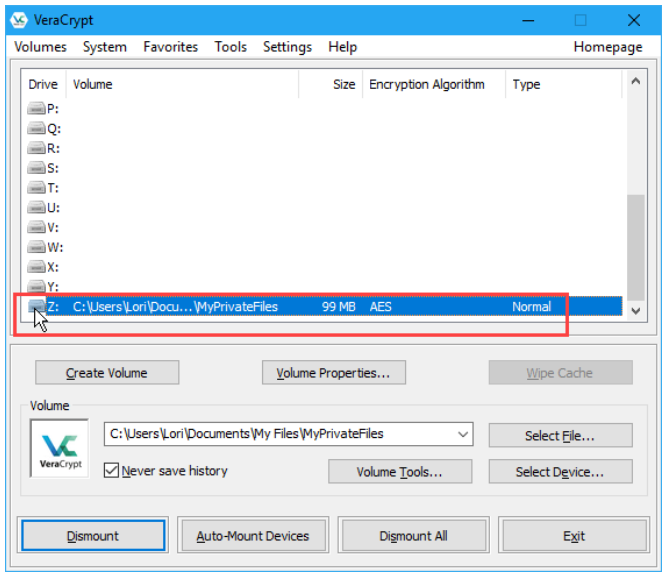
برای استفاده از Volume باید به اصطلاح آن را mount کنیم. برای این کار فایلی که قبلا برای Volume ساختیم را انتخاب می‌کنیم، یک درایو دلخواه را انتخاب کنید - مثلا درایو Z - و روی دکمه Mount کلیک کنید و رمز عبور ولوم را وارد کنید.



اگر یادتان هست که در هنگام ساخت ولوم از کدام الگوریتم رمزگذاری استفاده کرده‌اید، در قسمت PKCS-۵ PRF آن را انتخاب کنید و اگر آن را به یاد ندارید از گزینه پیش‌فرض Autodetection استفاده کنید. در این صورت ممکن است بازشدن ولوم کمی بیش‌تر زمان ببرد.

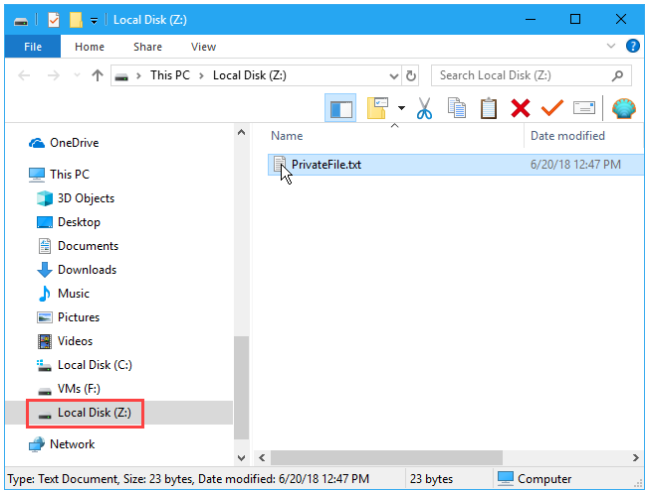


پس از این که ولوم با موفقیت روی سیستم سوار یا Mount شد، ولوم خود را به عنوان یک دیسک مجازی در کنار حرف انتخاب‌شده مشاهده خواهید کرد. برای دسترسی به ولوم، در VeraCrypt روی حرف آن دو بار کلیک کنید.

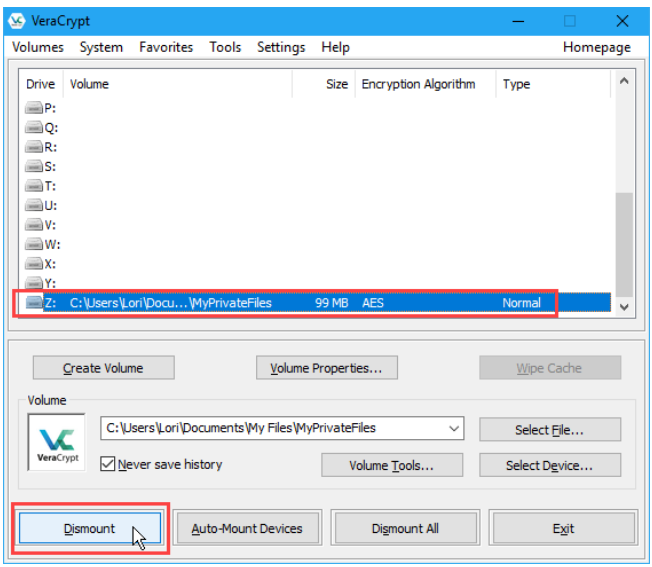


همچنین می‌توانید از مرورگر فایل برای کاوش در ولوم استفاده کنید که تفاوتی با سایر ولوم‌ها و دیسک‌ها نخواهد داشت. برای مثال ما ولوم VeraCrypt را در حرف Z سوار کرده‌ایم و با همان حرف نیز در مرورگر فایل نمایش داده شده است.

VeraCrypt هرگز داده‌های رمزگشایی‌شده را در دیسک شما ذخیره نخواهد کرد و فقط از حافظه RAM استفاده می‌کند. حتی زمانی که ولوم را روی سیستم سوار می‌کنید هم داده‌های داخل آن رمزنگاری شده‌اند. به این ترتیب، هنگامی که با فایل‌های خود کار می‌کنید، رمزنگاری و رمزگشایی آن‌ها در لحظه صورت می‌گیرد.



پس از اتمام کار با Volume حتما می‌بایست Volume را Dismount کنیم.



برای سیستم عامل اندروید می‌توانید از اپ EDS Lite استفاده کنید که مشابه VeraCrypt است و می‌توانید فایل‌های ولوم تولیدشده با VeraCrypt را با آن باز کنید. در EDS Lite به ولوم‌ها، کانتینر (container) گفته می‌شود. بقیه موارد مشابه است.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام دسته از ابزارهای زیر، به‌طور پیش‌فرض از رمزگذاری end-to-end پشتیبانی می‌کنند؟

الف) بله، زوم، تلگرام.

ب) تلگرام، مسنجر فیس‌بوک، اسکایپ.

ج) سکرت‌چت تلگرام، سیگنال، واتس‌اپ.

د) مسنجر فیس‌بوک، تلگرام، بله.

۲- کدام توصیه برای فعالان و معترضان درست است؟

الف) رمزگذاری مدارک و فایل‌های مهم، در کامپیوتر شخصی که دیگران دسترسی ندارند، ضروری نیست.

ب) رمزگذاری مدارک و فایل‌های مهم، برای ذخیره آن‌ها ضروری است.

ج) رمزگذاری مدارک و فایل‌های مهم، فقط موقع استفاده از وای‌فای عمومی ضروری است.

د) رمزگذاری مدارک و فایل‌های مهم، فایده‌ای ندارد. چون رمز آن‌ها را می‌توان پیدا کرد.

۳- تفاوت اصلی بین رمزگذاری متقارن و نامتقارن چیست؟

الف) رمزگذاری متقارن از کلید یکسان برای رمزگذاری و رمزگشایی استفاده می‌کند، در حالی که رمزگذاری نامتقارن از کلیدهای مختلف استفاده می‌کند.

ب) رمزگذاری متقارن همیشه ضعیف‌تر از رمزگذاری نامتقارن است.

ج) رمزگذاری متقارن برای ایمیل‌ها استفاده می‌شود، و رمزگذاری نامتقارن برای وب‌سایت‌ها.

د) رمزگذاری متقارن کندتر از رمزگذاری نامتقارن است.

درس پنج
امنیت سایبری، ۵: عکس و فیلم‌برداری امن و ارسال امن محتوا

در آبان ۱۴۰۱ نشریه آمریکایی اینترسپت (The Intercept) یک گزارش تحقیقی راجع به روش‌های نظام در رصد دستگاه‌های تلفن همراه را منتشر کرد. این گزارش نشان می‌دهد که حکومت ایران از ابزارهای پیشرفته‌ای برای کنترل و رصد ارتباطات تلفن همراه استفاده می‌کند، سیستمی به نام «سیام» که توسط سازمان تنظیم مقررات و ارتباطات رادیویی ایران تحت نظر حکومت اجرا می‌شود، امکاناتی چون کنترل سرعت انتقال داده‌ها، رمزگشایی تماس‌ها و مکالمات، ردگیری مسیر تردد افراد از طریق سیستم آنتن‌های BTS اپراتورهای موبایل، و دسترسی به جزئیاتی از ارتباطات کاربران را فراهم می‌کند.

این سامانه از طریق کنترل اپراتورهای موبایل، قابلیت صدور دستورات از راه دور برای تغییرات، ایجاد اخلال و رصدکردن رفتار کاربران را می‌دهد. از طریق این سیستم، حکومت می‌تواند به طور دقیق مکان و زمان تماس‌ها را کنترل کرده و حتی جزئیاتی از مکالمات و ارتباطات شخصی کاربران را دسترسی پیدا کند.

این نوع کنترل و رصد ارتباطات تلفن همراه، در برابر اعتراضات و فعالیت‌های مخالفان حکومت، به عنوان ابزاری برای خاموش‌کردن اعتراضات و کنترل رفتار معترضان مطرح

می‌شود.

عدم رعایت نکات امنیت سایبری می‌تواند ما را در معرض رصد سیستم امنیتی قرار دهد و حتی باعث دستگیری و تشکیل پرونده قضایی برایمان شود.

با توجه به این موارد و مواردی که در درس‌های قبل مطرح کردیم، اگر قصد مخفی‌ماندن و عدم ردگیری توسط سازمان‌های امنیتی رژیم در حین شرکت در تظاهرات و تجمعات اعتراضی دارید، به هیچ وجه نباید تلفن همراه ثبت‌نام‌شده با نام خودتان را در به صورت روشن در تظاهرات ببرید. دقت کنید که حتی اگر سیم کارت تلفن را هم خارج کنید، سیستم مخابراتی می‌تواند با ردگیری شماره IMEI دستگاه تلفن - اگر دستگاه با نام شما ثبت شده باشد - و ترددتان را در زمان‌های مختلف رصد کند. بنابراین اگر لازم است با خود دستگاه تلفن حمل کنید، در صورت امکان یک دستگاه تلفن بی‌نام‌ونشان تهیه کنید و آن را با خود به تجمعات ببرید.

برخی از دکه‌ها و فروشگاه‌های موبایل، تلفن‌های ثبت‌نام‌شده و سیم‌کارت بی‌نام یا به نام آدم‌های جعلی، به خریداران ارائه می‌کنند. بهتر است شما هم یک موبایل و یک سیم‌کارت بی‌نام‌ونشان داشته باشید. نکته مهم این‌که هرگز این موبایل بی‌نام نمی‌بایست مدت زمان طولانی در کنار موبایل اصلی شما روشن باشد، به این دلیل که سیستم اطلاعاتی با ردگیری موبایل‌های مشکوک می‌تواند، دستگاه‌هایی که در مدت زمان مشخص در نزدیکی آن موبایل روشن بوده‌اند را شناسایی کند و با این کار هویت شما لو می‌رود.

از سویی مطمئن باشید اطلاعاتی که در دستگاه تلفن همراهتان هست، منجر به شناسایی شما نمی‌شود. می‌توانید در اپ‌های مناسب، حساب‌های کاربری غیرواقعی بسازید و یک وی.پی.ان امن برای ارتباط‌گیری آنلاین و همین‌طور یک پیام‌رسان آفلاین را در این دستگاه از قبل نصب کنید.

توصیه اکید می‌شود که اپلیکیشن Bridgefy را در موبایل خود نصب کنید و به تمام دوستان همراهتان خودتان هم توصیه کنید آن‌ها نیز این اپ را نصب کنند. در این صورت هنگام قطع کلی یا منطقه‌ای اینترنت با این اپلیکیشن می‌توانید با دوستان و تمام کسانی که در اطراف شما این اپلیکیشن را نصب دارند، ارتباط داشته باشید.

حتما عکس و فیلم‌هایی که می‌خواهید به رسانه‌ها بفرستید را در شبکه Broadcast این اپلیکیشن ارسال کنید. با این کار احتمال انتشار تصاویر و فیلم‌ها بیش‌تر خواهد شد به

این دلیل که تعداد بیش‌تری آن را در اختیار خواهند داشت.

اگر با تعداد زیادی دوست در تجمعی شرکت کرده‌اید، در صورت قطع کامل یا منطقه‌ای اینترنت، یک یا چند نفر از شما در یک نقطه امن مثل داخل رستوران یا فروشگاه یا مرکز خرید نزدیک به محل مستقر شوید و فیلم و عکس‌هایی که توسط سایر دوستان تهیه می‌شود را با Bridgefy برای آن‌ها بفرستید تا در صورت دستگیری افراد در صحنه، این فیلم‌ها و عکس‌ها قابلیت پخش در ساعت‌ها و روزهای آتی را داشته باشند.

۷ نکته ضروری برای فیلمبرداری و عکسبرداری از اعتراضات

۱. ماموران امنیتی - چه رسمی‌ها و چه لباس‌شخصی‌ها - روی کسانی که از صحنه‌های تظاهرات فیلم و عکس می‌گیرند متمرکز می‌شنود و سعی می‌کنند آن‌ها را شناسایی کنند. بنابراین حتما چهره خود را بپوشانید. در درس‌های بعدی درباره روش‌های موثر پوشاندن چهره و نحوه لباس‌پوشیدن در اعتراضات بیش‌تر توضیح می‌دهیم.

۲. منطقه تظاهرات و تجمع را از قبل شناسایی کنید و راه‌های فرار و مناسب‌ترین نقطه برای عکسبرداری و فیلمبرداری را از پیش انتخاب کنید. سعی کنید از نماهایی تصویر بگیرد که حجم جمعیت و رفتار ماموران در تصویر قرار بگیرد.

۳. به هیچ وجه در تظاهرات از خود سلفی نگیرید، شاید مجبور شوید حین فرار از دست ماموران دوربین یا دستگاه تلفن همراه خود را دور بیندازید، همان‌طور که قبلا گفتم در دستگاهی که حمل می‌کنید، نباید چیزی پیدا شود که هویت شما به واسطه آن شناسایی شود.

۴. سعی کنید در تجمعات از صورت افراد فیلم و عکس نگیرید، قبل از ارسال فیلم یا عکس به رسانه‌ها، یک بار آن را مرور کنید و اگر صورت شخصی به صورت واضح مشخص بود آن قسمت‌ها را به وسیله اپ‌های ادیت عکس و ویدیو محو یا شطرنجی کنید.

۵. در تظاهرات‌های اخیر نیروهای لباس‌شخصی گاهی خود را معترض جا می‌زدند و در نقاطی که به ماموران امنیتی نزدیک بود، با معترضان همراهی می‌کردند و با این ترفند در یک حرکت غافلگیرکننده، معترضانِ به قول خودشان موثر را به سمت ماموران هل می‌دادند و باعث دستگیری آن‌ها می‌شدند. بنابراین سعی کنید در نقاط

نزدیک به ماموران امنیتی قرار نگیرید و حرکت‌های مشکوک معترض‌نماها را رصد کنید.

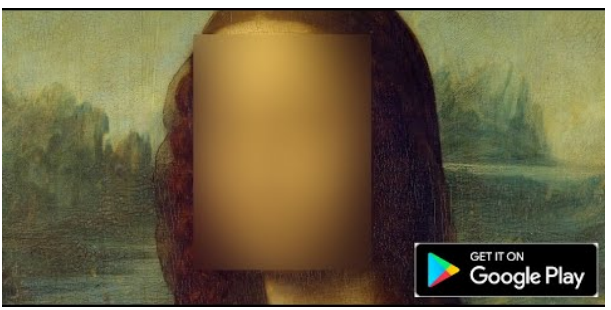
۶. اگر به جای دستگاه تلفن همراه از دوربین‌های کوچکی که می‌تواند در لباس‌تان مخفی شوند استفاده کنید و امکان این‌که ماموران روی شما تمرکز کنند را کم کرده‌اید، هرچند ارسال این‌گونه فیلم و عکس‌ها مخصوصا اگر دوربین قدیمی که به موبایل وصل نباشد، در حین تظاهرات به‌راحتی امکان‌پذیر نیست.

اگر در موقعیتی قرار گرفتید که می‌دانید به احتمال زیاد دستگیر می‌شوید، و امکان رساندن موبایل یا دوربین، به دوستان در موقعیت بهتر برایتان میسر نیست، در صورت امکان موبایل را به تنظیمات کارخانه‌ای برگردانید و آن را دور بیاندازید. در صورتی که پس از دستگیری بازجو خواست شما مالکیت آن موبایل را به عهده بگیرید، به کل منکر شوید

معرفی ابزارهای محوکردن تصاویر و فیلم‌ها

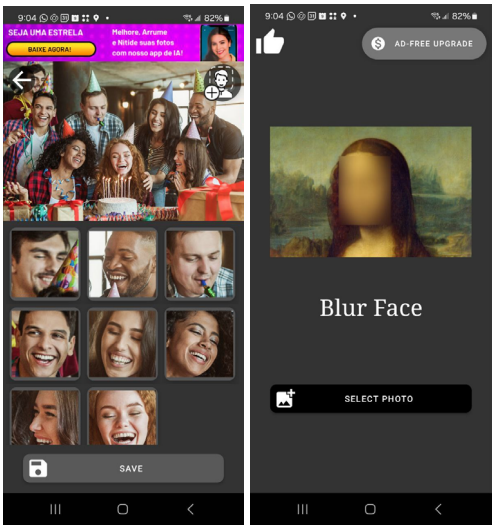
اپ‌های بی‌شماری برای مات‌کردن چهره‌ها در عکس‌ها وجود دارند که برخی حرفه‌ای و برخی بسیار ساده هستند. در ادامه یکی از ساده‌ترین اپ‌های مات‌کردن را برای موبایل‌های اندروید معرفی می‌کنیم و نحوه کار با آن را توضیح می‌دهیم.

Blur Face: ۱ Tap Photo Censor



روش کار

پس از دانلود و نصب برنامه را باز می‌کنیم، روی گزینه select photo تپ کرده و عکس خود را انتخاب می‌کنیم.



با این کار، نرم‌افزار به طور خودکار تمام چهره‌ها را شناسایی می‌کند و در پایین تصویر نشان می‌دهد. در این مرحله روی هر بخش از تصویر کوچک در پایین که بزنیم، آن صورت در تصویر بالا مات خواهد شد. اگر از میزان مات‌شدن تصویر راضی نبودید، دوباره روی آن بزنید! بعد هم روی گزینه Save بزنید. این اپ رایگان است ولی حین اجرای اپ تبلیغات در آن خواهید دید.

محوکردن صورت در فیلم با Inshot

ابزارهای بسیار زیادی برای ویرایش فیلم وجود دارد که یادگیری نحوه مات‌کردن در آن‌ها چندان سخت نیست. یکی از آسان‌ترین این اپ‌ها برای اندروید و اپل اپ Inshot است.

این اپ نیز به صورت رایگان ارائه شده است، اما احتمال پخش تبلیغات در آن وجود دارد. لازم به یادآوری است که از این ابزار برای ادیت عکس هم می‌شود استفاده کرد. نحوه استفاده از این اپ را می‌توانید در این ویدیو ببینید.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- حتی اگر سیم کارت تلفن را هم خارج کنید، اگر گوشی تلفن شما به نام‌تان ثبت شده باشد، سیستم مخابراتی می‌تواند با ردگیری شماره IMEI دستگاه تلفن، تردد شما را رصد کند.

الف) درست است.

ب) نادرست است.

ج) فقط در شهرهای بزرگ ممکن است.

د) فقط در مناطق روستایی ممکن است.

۲- کدام توصیه برای شرکت در تظاهرات، درست است؟

الف) مشکلی نیست اگر فقط از خود و دوستان‌مان، عکس سلفی بگیریم.

ب) حتما چهره خود را بپوشانیم.

ج) مشکلی نیست اگر عکس‌های شامل چهره واضح خود یا دیگران را برای رسانه‌هایی که دنبال‌کننده زیاد دارند، بفرستیم.

د) مشکلی نیست اگر عکس‌های شامل چهره واضح خود یا دیگران را برای دوستان و آشنایان، بفرستیم.

۳- اگر در تظاهرات در موقعیتی هستید که به‌زودی بازداشت می‌شوید، بهتر است گوشی تلفن خود را...

الف) خاموش کنید.

ب) به تنظیمات کارخانه بازگردانید و آن را دور بیندازید.

ج) در حالت هواپیما قرار دهید.

د) اینترنت و بلوتوث را سریع خاموش کنید.

درس شش
اعتراضات، ۱: روند دادرسی یک پرونده در دستگاه قضایی

شرکت در تجمعات اعتراضی در جمهوری اسلامی یعنی قبول خطر دستگیری و تشکیل پرونده قضایی. فرایند دستگیرشدن، حتی برای کسانی که بارها سابقه بازداشت‌شدن دارند، فرایندی پراسترس و ترسناک است. بنابراین آشنایی مختصر با دستگاه قضایی، قوانین مربوط به آن و دانستن حق و حقوق قانونی، به بهبود شرایط روحی و اعتمادبه‌نفس شخص، در مواجهه با این شرایط، کمک فراوانی می‌کند.

قانون اساسی جمهوری اسلامی، اصل ۲۷ قانون اساسی، تجمعات آزاد را مشروط به عدم حمل سلاح و نبودن مخل مبانی اسلام، به رسمیت شناخته است. یعنی این‌که قانون اساسی، حق تجمعات اعتراضی مسالمت‌آمیز و بدون خشونت را به رسمیت شناخته است. این‌که نهادهای امنیتی و قضایی با بهانه غیرقانونی‌بودن یک تجمع، یا نداشتن مجوز برای یک تجمع، به سرکوب آن می‌پردازند نقض قانون اساسی است.

در ادامه ۷ ماده-قانون مورد استفاده در اغلب پرونده‌های فعالان سیاسی و مدنی که در تجمعات دستگیر می‌شوند، را بررسی می‌کنیم.

۷ ماده-قانون مورد استفاده در اغلب پرونده‌های فعالان سیاسی و مدنی

۱- ماده ۵۰۰: تبلیغ علیه نظام - یک سال حبس: از نظر دادگاه انقلاب هر گونه انتقاد به سیستم یا شعار در مخالفت با وضعیت موجود یا مصاحبه با رسانه‌های خارجی می‌تواند تبلیغ علیه نظام در نظر گرفته شود.

۲- ماده ۶۱۰: هرگاه دو نفر یا بیش‌تر اجتماع و تبانی کنند که جرایمی ضد امنیت داخلی یا خارج کشور مرتکب شوند یا وسایل ارتکاب آن را فراهم کنند، در صورتی که عنوان «محارب» بر آنان صادق نباشد، به ۲ تا۵ سال حبس محکوم خواهند شد. برای مثال در سال ۱۳۸۸ تقریبا از هر کسی اس.ام.اس یا ایمیلی گرفته بودند که دعوت به تظاهرات در آن بود، با این مورد اتهامی روبرو بود. هر عملی که توسط دو نفر یا بیش‌تر صورت بگیرد و با مزاج ضابط قضایی جور در نیاید، می‌تواند با این موارد اتهامی مواجه شود. شرکت در تظاهرات اگر با هماهنگی دو نفر صورت گرفته باشد از نظر دادگاه انقلاب مشمول این ماده می‌شود.

۳- ماده ۶۹۸: تشویش اذهان عمومی یا نشر اکاذیب- تا دو سال: دایره این ماده، مثل «تبلیغ علیه نظام»، در دادگاه انقلاب گسترده است. بیان هر خبری که از سوی نظام سانسور شده باشد، ارسال عکس و خبر و فیلم از تظاهرات به رسانه‌ها، می‌تواند تشویش اذهان عمومی یا نشر اکاذیب محسوب شود.

۴- ماده ۵۱۴: توهین به رهبر و روح‌الله خمینی- دو سال حبس: از نظر دادگاه انقلاب هر حرف و سخن و انتقاد به علی خامنه‌ای، رهبر جمهوری اسلامی، در زمره توهین حساب می‌شود. شما یا نباید راجع به خامنه‌ای و خمینی صحبت کنید یا در صورت صحبت فقط باید تعریف و تمجید کنید. شعار «مرگ بر دیکتاتور» و سایر شعارهای مرتبط به خامنه‌ای در تظاهرات، معمولا با کیفرخواستِ این ماده، مواجه می‌شود، که به عبارتی تایید نظر شعاردهنده در خصوص دیکتاتوربودن خامنه‌ای است!

۵- ماده ۶۰۹: توهین به مقامات - یعنی رییس جمهور به پایین- شش ماه حبس: دامنه این ماده هم خیلی گسترده است و هرگونه شعار علیه مقامات جمهوری اسلامی را شامل می‌شود.

۶- ماده ۲۸۶: افساد فی‌الارض: «هرکس به طور گسترده مرتکب جنایت علیه تمامیت جسمانی افراد، جرایم علیه امنیت داخلی یا خارجی کشور، نشر اکاذیب، اخلال در نظام

اقتصادی کشور، احراق و تخریب، پخش مواد سمی و میکروبی و خطرناک یا دایرکردن مراکز فساد و فحشا یا معاونت در آن‌ها شود، به‌گونه‌ای که موجب اخلال شدید در نظم عمومی کشور، ناامنی یا ورود خسارت عمده به تمامیت جسمانی افراد یا اموال عمومی و خصوصی یا سبب اشاعه فساد و فحشا در حد وسیع شود، مفسدفی‌الارض محسوب و به اعدام محکوم می‌شود.» همان‌طور که می‌بینید دایره تعریف «مفسدفی‌الارض» هم گسترده است. بنا به میل ضابط قضایی و قاضی و بر مبنای علم قاضی می‌تواند شامل خیلی از افراد شود.

۷- ماده ۲۷۹: محاربه: هر کس که برای ایجاد رعب و وحشت و سلب امنیت و آزادی مردم دست به اسلحه ببرد، «محارب فی الارض» است.

۷ واژه قضایی پروسه دادرسی در پرونده‌های امنیتی

۱- ضابط قضایی یا کارشناس پرونده

نیروهای امنیتی و انتظامی در سیستم قضایی، ضابط قضایی نامیده می‌شوند. در کل ضابط قضایی بدون حکم بازداشت که در آن اتهام شخص به طور مشخص ذکر شده باشد، اجازه دستگیری کسی را ندارد. معمولا اگر توسط نهادهای امنیتی دستگیر شده باشید، ضابطین قضایی اسم مستعار دارند و خود را کارشناس پرونده معرفی می‌کنند.

۲- قاضی بازپرس، قاضی دادیار و دادستان پرونده

کسی است برای شما نوع قرار تامین کیفری را تعیین می‌کند و بر اساس گزارشاتِ ضابط قضایی برای شما کیفرخواست تهیه می‌کند و برای دادرسی به دادگاه می فرستد. معمولا اگر حین بازجویی اعترافی کردید و بر اساس آن اتهامی به شما نسبت داده شده باشد، آن بازجویی می‌بایست در حضور دادیار یا بازپرس پرونده تکرار شود. در صورت قبول یک اتهام در اثر فشار بازجویی، حتما در جلسه دادیاری یا بازپرسی آن را بیان کنید و به صورت کتبی بنویسید که در اثر فشار و شکنجه بازجویی مجبور به قبول این اتهام شده‌اید.

نکته: در نظر داشته باشید که دادگاه هیچ گاه ادعای شما در خصوص اعتراف اجباری تحت فشار، در مواردی که در بازجویی قبول کرده و در جلسه دادیاری یا بازپرسی هم قبول کرده باشید، را نمی‌پذیرد.

۳- قرار کیفری و انواع آن

به منظور دسترسی به متهم و حضور به موقع او، جلوگیری از فرار یا مخفی‌شدن او، و

تضمین حقوق بزه‌دیده، برای جبران ضرر و زیان او، دادیار، بازپرس یا دادستان، پس از تفهیم اتهام و تحقیق لازم، در صورت وجود دلایل کافی، یکی از انواع قرارهای تامین را صادر می‌کند. در واقع انواع مختلفی از قرارهای تامین از جمله «قرار با قول شرف» در قانون در نظر گرفته شده است ولی در پرونده‌های امنیتی معمولا یکی از ۳ قرار زیر استفاده می‌شود:

- **بازداشت موقت:** همان‌طور که از اسمش پیداست موقت است و رمان رسیدگی به آن‌ها، که در صلاحیت دادگاه‌های کیفری عمومی یا اختصاصی است، دو ماه در نظر گرفته شده است؛ البته به شرطی که مدت حبس از حداقل مجازاتِ مقررِ قانونیِ جرمِ ارتکابی، تجاوز نکند. یعنی اگر برای یک جرمی که برای آن ۶ ماه تا ۳ سال حبس در نظر گرفته شده است، مدت بازداشت موقت نباید بیش‌تر از ۶ ماه باشد.
- **اخذ وثیقه:** وثیقه اعم از وجه نقد، ضمانت‌نامه بانکی، مال منقول یا غیرمنقول است. در این قرار از قرارهای تامین کیفری، متهم، مالی را در ازای بازداشت‌نشدن، به دادگاه می‌سپارد که به آن، وثیقه می‌گویند.
- **اخذ کفیل با تعیین وجه‌الکفاله:** در این قرار تامین که به آن قرار کفالت می‌گویند، متهم، شخص ثالثی را به عنوان کفیل، به دادگاه معرفی می‌کند و کفیل، بازگرداندن متهم را با سپردن مبلغی که به آن وجه‌الکفاله می‌گویند، تضمین می‌کند و به این ترتیب، متهم، بازداشت نمی‌شود.

  نکته: در بسیاری از پرونده‌های امنیتی، برای این‌که شکل دادرسی عادلانه به نظر بیاید، قرار وثیقه یا کفالت توسط دادستانی صادر می‌شود ولی به متهم یا خانواده ابلاغ نمی‌شود و بازپرس یا دادیار پرونده در پرونده می‌نویسند: «عجز در تودیع وثیقه»! یعنی دروغ می‌نویسد و به نوعی دست ضابط قضایی یا بازجو را برای اعمال فشار بیش‌تر با طولانی‌کردن زمان بازداشت، باز می‌گذارد.

۴- دفاع آخر زمان بازپرسی: پس از پایان دوره بازجویی، برای دفاع آخر، شما را نزد بازپرس یا دادیار پرونده می‌برند. جواب‌هایی که در آن جلسه می‌دهید خیلی مهم است، حتما در جواب‌ها ذکر کنید تحت چه نوع فشارهایی بوده‌اید. مواردی مثل انفرادی طولانی مدت، نداشتن ارتباط با خانواده و وکیل، برخورد خشن و تند بازجو، تهدیدات روانی و شکنجه‌های فیریکی، دسترسی‌نداشتن به اخبار، چشم‌بند و توهین لفظی و انفرادی جز

موارد شکنجه محسوب می‌شود. لازم است این مورد به طور مشروح در دفاع آخر شما در بازپرسی ذکر شود.

۵- کیفرخواست: کیفرخواست همان ادعانامه دادستان است که پس از پایان تحقیقات مقدماتی در خصوص متهم صادر می‌شود. در اصل، بازپرس یا دادیار باید برای شما کیفرخواست صادر کنند. ولی این کار معمولا توسط ضابط قضایی یا همان نهاد امنیتی انجام می‌گیرد و بازپرس و دادیار فقط آن را امضا می‌کنند.

۶- دادگاه بدْوی و قاضی پرونده: در دادگاه بدوی، قاضی پرونده بر اساس دادخواست دادسرا که به امضای دادیار، بازپرس یا دادستان رسیده، به پرونده شما رسیدگی می‌کند و با توجه به دفاعیات شما و وکیل‌تان، دادخواست و محتویات پرونده و گزارشات بازجویی شما، برایتان حکم صادر می‌کند.

۷- دادگاه تجدید نظر یا دیوان عالی: پس از اعلام رأی دادگاه بدوی، بر اساس درخواست فرد متهم یا وکیل‌اش، پرونده به دادگاه تجدید نظر یا دیوان ارسال و آنجا پس از بررسی مجدد، حکم دادگاه بدوی را تایید، یا رد می‌کند یا برای بررسی، به یک شعبه دیگر - یعنی به شعبه هم‌عرض - ارسال می‌کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- پس از پایان بازجویی، هنگام آخرین دفاع نزد بازپرس یا دادیار، بهتر است حتما بگوییم تحت چه فشارها و شکنجه‌هایی بوده‌ایم.

الف) بله، فقط اگر بازپرس رفتار مهربانانه داشت.

ب) خیر، چون دیگر زمان این کار گذشته است.

ج) بله، کاملا درست است. باید بگوییم.

د: خیر، چون به ضررمان تمام می‌شود.

۲- ضابط قضایی یا کارشناس پرونده کیست؟

الف) عنوان دیگر قاضی دادگاه است.

ب) عنوان دیگر دادیار است.

ج) نیروهای امنیتی و انتظامی که مسئولیت بازداشت افراد را دارند.

د) عنوان دیگر دادستان پرونده است.

۳- کدام تعریف برای اتهام «تشویش اذهان عمومی یا نشر اکاذیب» درست است؟

الف) معادل توهین به رهبری و مقامات نظام است.

ب) ایجاد شبکه با دیگر افراد از طریق فروش نوشیدنی‌های الکی و دایرکردن مراکز فحشا.

ج) بیان محتوایی که از سوی نظام سانسور شده باشد یا ارسال عکس و خبر و فیلم از تظاهرات به رسانه‌ها.

د) شرکت در تجمعات اعتراضی و دیوارنویسی.

درس هفت
اعتراضات، ۲: استراتژی جلسات دادرسی و بازپرسی

گاهی جلسات دادیاری و بازپرسی در محل بازداشت و بیش‌تر مواقع در دفاتر دادیاری یا بازپرسی در دادسرا انجام می‌گیرد. بنابراین لازم است هوشیار باشید و بدانید که شخصی که از شما بازجویی می‌کند، ضابط قضایی است یا این‌که قاضی دادیار یا بازپرس است. ضابط قضایی مامور انتظامی یا نیروهای امنیتی است که معمولا خود را کارشناس پرونده معرفی می‌کنند.

دادیار و بازپرس کسی است که می‌تواند برای شما درخواست تغییر تامین قرار و تبدیل قرار بازداشت به وثیقه یا کفالت بکند. پس لازم است در تمامی جلسات دادیاری و بازپرسی، کتبا اعلام کنید که نیازمند به وکیل، تماس و ملاقات با خانواده هستید و درخواست تبدیل قرار تامین از بازداشت به وثیقه و کفالت دارید و همچنین این‌که خانواده قادر به تهیه وثیقه هستند را مکتوب بنویسید.و اگر بازپرس گفت که وثیقه صادر شده است و خانواده نتوانسته‌اند آن را تهیه کنند، در همان جا به صورت مکتوب تماس با خانواده و وکیل را درخواست کنید. یادتان باشد هر درخواستی باید مکتوب باشد و ترجیحا در برگه سوال و جواب بازپرس یا دادیار این موارد را ذکر کنید تا در پرونده ضبط شود.

اگر در انفرادی هستید یا توسط بازجو یا کارشناس پرونده تهدید شده‌اید، حتما در حضور دادیار یا بازپرس آن را مکتوب کنید و مرتب اذعان کنید که در بازداشتگاه، تحت

فشار بازجو یا همان کارشناس پرونده هستید و نحوه فشارها اعم از تهدیدات، شکنجه‌های روانی و فیزیکی را با شرح کامل در برگه‌های بازپرسی مکتوب کنید.

اگر تحت شکنجه باشید، مطمئن باشید این کار شما از فشارهای تیم بازجویی خواهد کاست. اگر در جلسات بازپرسی توانستید با اعضای خانواده یا وکیل‌تان دیدار داشته باشید - که این مورد خیلی نادر است - آن‌ها را از جزییات فشارهای دوران بازداشت آگاه کنید و بخواهید و تاکید کنید که پرونده‌تان را رسانه‌ای کنند. به این دلیل که تجربه ثابت کرده است فشار روی متهمانی که پرونده‌شان رسانه‌ای شده، به مراتب کم‌تر از سایر متهمان است. همچنین به حرف‌های بازجو و مقامات قضایی که از شما می‌خواهند برای فیصله‌یافتن زودتر پرونده، از رسانه‌ای‌کردن آن خودداری کنید، توجه نکنید و به یاد داشته باشید که بازجو و بازپرس دوست شما نیستند!

۸ نکته مهم درباره مستندات مورد استفاده در دادگاه‌های انقلاب

۱. بازجو یا بازپرس بایست بر اساس قوانین برای شما کیفرخواست صادر کنند. هر چیزی که حین بازجویی بیان می‌کنید، می‌تواند علیه خودتان در پرونده به کار گرفته شود

۲. بر اساس قوانین فعلی و رویه موجود در دادگاه انقلاب، مهم‌ترین مدرک برای اثبات جرم، اعتراف متهم است، حتی اگر به چیز غیر ممکنی هم اعتراف کنید، دادگاه انقلاب مثل دادگاه جنایی نیست که امکان‌سنجی کند. همان اعتراف برای صدور حکم کافی‌ست.

نکته: توجه کنید که نحوه دادرسی در پرونده‌های سیاسی-امنیتی با تمام جرائم دیگر تفاوت دارند. در دادرسی پرونده‌های سیاسی-امنیتی بسیاری از قوانین دادرسی رعایت نمی‌شود. برای اثبات وقوع عمل مجرمانه و نسبت‌دادن آن به متهم، باید دلایلی توسط مرجع تحقیق - یا همان بازجو یا کارشناس پرونده است - ارائه شود و در جریان دادرسی مورد بررسی و بحث قرار گیرند. در حقوق جمهوری اسلامی این دلایل شامل «اقرار»، «شهادت» و «علم قاضی» است.

۳. مهم‌ترین مدرک، علیه متهم در دادرسی در دادگاه‌های انقلاب اعتراف علیه خود است. هر اعترافی که در مرحله بازجویی از شما بگیرند و شما آن را در مرحله

بازپرسی، یعنی در حضور بازپرس یا دادیار پرونده تکرار کرده باشید، مدرکی علیه شما حساب می‌شود و حتی در صورت انکار در دادگاه، چون یک بار در حضور قاضی بازپرس به آن اعتراف کرده‌اید، مدرک معتبر علیه خودتان قلمداد می‌شود، حتی اگر این اعتراف علیه خودتان از نظر فنی و منطقی امکان‌ناپذیر باشد! برای مثال یک پیرمردِ از دو پا فلج، که بدون عصا نمی‌توانست راه برود، در اعتراضات سال ۸۸ به اتهام تخریب و به‌آتش‌کشیدن چندین اتوبوس محکوم شده بود!

۴. ۴-امارات قضایی یعنی چیزهایی که در نظر قاضی می‌توانند نشانه وقوع یا عدم وقوع جرمی باشند. این مورد هم می‌تواند استناد قاضی برای صدور حکم باشند و از موارد علم قاضی به حساب بیاید. مدارکی چون صدای ضبط‌شده، فیلم، عکس، نتایج تست‌های و موارد مشابه آن، همگی از جمله این موارد هستند.

۵. ارزش نوع مدارک بسته به نظر بازجو و قاضی دارد. فیلم، عکس و صدای ضبط‌شده در حال حاضر با توجه به این‌که نسبت‌دادن آن به فرد، قابل اثبات نیست از امارات قوی محسوب نمی‌شوند و متهم به‌راحتی می‌تواند منکر ارتباط خود با آن‌ها شود. به طور نمونه حتی اگر عکس یا فیلم فردی به طور واضح در تظاهرات وجود داشت، متهم می‌تواند از پذیرفتن این که عکس داخل پرونده از او است، خودداری کند به خصوص این‌که ساختن عکس یا فیلم‌های ساختگی با استفاده از فتوشاپ یا سایر نرم‌افزارها و هوش مصنوعی بسیار راحت شده است. در این صورت دادگاه برای محکومیت متهم باید در کنار عکس و فیلم، دلایل دیگری هم داشته باشد. مثلا عکس همراه با دوستان یا خانواده فرد باشد یا در دستگاه‌های هوشمند یا کامپیوتر شخصی متهم پیدا شده باشد و متهم به این‌که صاحب آن کامپیوتر شخصی است هم اعتراف کرده باشد.

۶. به‌دست‌آمدن فیلم، ویدیو و نوشته از شما که حاوی انتقاد به وضعیت کشور، انتقاد به مسئولان نظام یا تشویق دیگران به اعتراض به وضعیت موجود باشد، تنها در صورتی که در مراحل بازجویی و بازپرسی مورد تایید شما قرار بگیرد، می‌تواند مدرکی علیه شما قلمداد شود. تاکید می‌کنیم که اگر بازجو مدرکی از شما به دست آورده باشد، این مدرک وقتی برای دادگاه سندیت دارد که شما اعتراف کنید آن مدرک مربوط به شما ست و این اعتراف وقتی قطعی است که در مرحله بازپرسی و دادیاری در حضور قاضی بازپرس و دادیار به آن اعتراف کرده باشید. برای بار چندم تکرار می‌کنیم

اگر در حضور بازپرس و دادیار چیزی را قبول کنید، انکارش در دادگاه انقلاب دیگر بی‌فایده خواهد بود.

۷. مطالب مربوط در ایمیل، فیس‌بوک، تلگرام، اینستاگرام و سایر اپ‌ها و شبکه‌های اجتماعی - حتی نوشتن یک کامنت - از مواردی است که در حال حاضر در دادگاه انقلاب مورد استناد دادگاه‌ها قرار می‌گیرد. برای این منظور اولا ضابط قضایی باید ثابت کند که ایمیل یا صفحه مربوطه در شبکه‌های اجتماعی یا کامنت، متعلق به متهم است و ثانیا باید ثابت کند اظهارات بیان‌شده در این موارد جنبه مجرمانه دارد. همچنین با توجه به آن که امکان هک‌کردن ایمیل و ورود به ایمیل دیگر افراد وجود دارد باید ثابت کنند که مطلب مذکور را متهم شخصا نوشته است.

۸. شما می‌توانید در بازجویی و بازپرسی ادعا کنید که افراد دیگر با هک‌کردن شما و به‌دست‌آوردن پسورد شخصی‌تان وارد ایمیل، فیس‌بوک و دیگر ابزارهای ارتباطاتی شما شده‌اند و اصلا خودتان از آن اطلاع نداشته‌اید.

ثبت نام در سامانه «ثنا» و در دسترسی فرد مورد اعتمادتان به آن حساب

قوه قضائیه جمهوری اسلامی، اقدام به راه‌اندازی سامانه‌ای با عنوان «ثنا» کرده است. کاربران از طریق این سیستم دولتی می‌توانند به شکل آنلاین و اینترنتی به کلیه ابلاغ‌های قضایی، اوراق، دادخواست‌ها و شکوائیه‌های خود دسترسی داشته باشند. به این ترتیب؛ برخلاف روش‌های سنتی گذشته با ثبت ثنا، مشکلات عدم دریافت به‌موقع احضاریه یا اخطاریه به فرد و امثال آن، به کلی رفع شده است. همچنین با ثبت نام در سیستم ثنا با یک تلفن همراه که به نام خودتان ثبت شده است، به یک امضای الکترونیکی دسترسی خواهید داشت که می‌شود با آن حتی به یک وکیل برای پرونده خود وکالت دهید.

اگر احتمال این را می‌دهید که در تظاهرات دستگیر شوید، به یکی از دفاتر خدمات الکترونیک قضایی مرکز استان یا شعبه‌های دادگستری شهرستان محل سکونت‌تان مراجعه کنید. لازم است از قبل مدارکی چون کارت ملی، شناسنامه و یکی از قبوض آب، برق یا گاز خود را نیز همراه داشته باشید. در آنجا با داشتن یک تلفن موبایل به نام خودتان می‌توانید یک حساب آنلاین در سیستم ثنا ثبت کنید.

برای ورود به این سیستم نیاز به تلفن همراهتان است. تمامی موارد مربوط به ثبت نام

و همچنین دسترسی موبایل خود را به یکی از اقوام نزدیک مورد اعتماد بدهید و در این صورت پس از دستگیری، کلیه ابلاغات قضایی از جمله صدور قرار وثیقه و امثال آن در این سیستم توسط فرد مورد اعتماد شما در دسترس است. همچنین با دراختیارداشتن حساب ثنا و دسترسی به امضای الکترونیکی شما، شخص مورد اعتمادتان می‌تواند به یک وکیل برای پیگیری پرونده شما وکالت دهد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- سامانه ثنا چیست؟

الف) سامانه مربوط به امور سجلی زندانیان سیاسی و عقیدتی که برای تایید هویت متهم در بازجویی استفاده می‌شود.

ب) سامانه‌ای مربوط به قوه قضاییه که امکان مشاهده ابلاغیه‌های قضایی، اطلاع‌رسانی پرونده و جزئیات شکواییه‌ها و دادخواست در آن فراهم است.

ج) سامانه‌ای مربوط به جرایم امنیتی‌ای که زندانیان سیاسی و عقیدتی مرتکب شده‌اند.

د) سامانه‌ای مربوط به هر امر دولتی زندانیان سیاسی و عقیدتی.

۲- «تهدیدها و شکنجه‌های روانی و فیزیکی توسط بازجو/کارشناس پرونده را باید در حضور دادیار یا بازپرس پرونده مکتوب شرح دهیم.» کدام گزینه درباره عبارت بالا، درست است؟

الف) فقط شکنجه‌های فیزیکی کافی است.

ب) بله، همه فشارها و تهدیدها و شکنجه‌ها را باید مکتوب شرح دهیم.

ج) نه، مکتوب لازم نیست. شفاهی کافی است.

د) فقط در صورتی که دادیار یا بازپرس گفتند که پیگیری و با بازجویان برخورد می‌کنند.

۳- امارات قضایی یعنی...

الف) اماکن مربوط به قوه قضائیه.

ب) پرونده متهم در سامانه ثنا.

ج) چیزهایی که در نظر قاضی می‌توانند نشانه وقوع یا عدم وقوع جرمی باشند.

د) اعتراف علیه خود مقابل دوربین و قاضی.

درس هشت
اعتراضات، ۳: نیروهای سرکوب‌گر، دوران بازجویی و بازداشت

هنگامی که با سیستم امنیتی رژیم مواجه می‌شوید و احتمال دستگیری‌تان وجود دارد، آشنایی با روش‌های بازجویی و ترفندهای این سیستم، همچنین استراتژی‌هایی برای سپری‌کردن دوره بازداشت، می‌تواند به شما کمک کند تا این دوران را با کمترین آسیب و مشکلات ممکن طی کنید.

دوران بازداشت موقت، دوران بسیار سختی است و باید خودتان را برای بدترین شرایط آماده کنید. در این دوران ارتباط شما با جهان بیرون از بازداشتگاه و اتاق بازجویی بسیار محدود و گاهی برای مدت‌های طولانی قطع می‌شود. در نظر داشته باشید که وظیفه هر بازجو این است که پرونده شما را هر چقدر که ممکن است سنگین‌تر کند. و در این راستا انواع و اقسام روش‌ها و متدها را به کار می‌گیرند.

هیچ گاه فراموش نکنید که هدف بازجو چیست؟ بازجوی خوش‌برخورد که با شما رفتاری دوستانه دارد، اغلب مواقع خطرناک‌تر از بازجوی خشن و بد رفتار است. هدف بازجو در پرونده‌های امنیتی، شکستن روحیه شما و مجبورکردن شما به اعتراف درباره اتهامات و افشای اطلاعات دوستان‌تان است.

فراموش نکنید که هر چه بیش‌تر اعتراف کنید و دوستان خود را در معرض خطر قرار دهید، پرونده خودتان را سنگین‌تر کرده‌اید، و دوران حبس طولانی‌تری خواهید داشت.

۴۵ نکته درباره بازجویی و بازداشت برای فعالان

۱. یک بازجو، حتی خوش‌رفتارترین، آن‌ها به هیچ وجه دوست شما نیست.
۲. هدف بازجو سنگین‌ترکردن پرونده شما به هر روش ممکن است.
۳. بازجو گاهی با روی خوش و دلسوزنشان‌دادن خود و با هم‌صحبتی با شما، مخصوصا وقتی مدت طولانی در انفرادی هستید، سعی در شکستن روحیه شما و دستیابی به اعتراف‌تان برای سنگین‌ترکردن پروند شما دارد.
۴. یک بازجوی خشن از توهین و شکنجه‌های روانی و فیزیکی استفاده می‌کند و هدف از این کارش ترساندن شما ست.
۵. اگر بازجوی خشن بفهمد که شما از شکنجه روحی و جسمی می‌ترسید، بلا استثنا، فشار روحی و جسمی را بیش‌تر می‌کند و این فشارها، روزبه‌روز تا جایی که به او ثابت کنید که دیگر شکنجه تاثیری بر شما ندارد، بیش‌تر خواهد شد.
۶. بازجویی، یک بازی روانی است که مهم‌ترین هدف آن اولا گرفتن اطلاعات از شما و ثانیا سنگین‌ترکردن پرونده و زیادترکردن اتهامات در پرونده شما است.
۷. بازجوها معمولا از روش سعی و خطا استفاده می‌کنند. اگر از یک روش نتوانند از شما حرف بکشند، روش دیگری را امتحان می‌کنند.
۸. معمولا ادعا می‌کنند که همه چیز را می‌دانند و فقط می‌خواهند از خودتان اعتراف بگیرند تا کمکی به حال شما باشند. در حالی که هر نوع همکاری با آن‌ها به ضرر شما خواهد بود.
۹. گاهی دست‌خط تک‌نویسی دیگران علیه شما را نشان می‌دهند تا شما را تحریک کرده و تشویق به تک‌نویسی کنند. هرگز در این دام نیفتید.
۱۰. ممکن است مدارکی علیه شما به شما نشان دهند؛ یادتان باشد مدارک وقتی معتبر است که با اعتراف شما همراه شود.
۱۱. تغییر بازجو و بازی بازجوی خوب و بازجوی بد، یک روشی است که تقریبا برای همه

اتفاق می‌افتد. یک بازجو ممکن است جلوی شما به بازجوی قبلی فحش هم بدهد و خود را حامی شما معرفی کند. با شما درد دل کند و مهربان باشد. فراموش نکنید که این‌ها بازی است و هر چیزی پیش هر کدام بگویید علیه‌تان استفاده می‌شود.

۱۲. تقریبا هر چیزی بازجو می‌گوید دروغ است. پیش‌فرض شما از صحبت‌های او باید این باشد که هر چیزی بگویند، دروغ است. دروغ‌هایی از قبیل «از فلان چیز خبر داریم»، «می‌خواهیم از خودت بشنویم»، «فلانی را دستگیر کرده‌ایم» و «او همه چیز را گفته» و از این دست جمله‌ها.

۱۳. در موارد خاص، این دروغ‌گویی حتی با سناریوهای روانی خاصی همراه می‌شود. مثلا از اتاق کناری صحبت‌های شخصی علیه خودتان را می‌شنوید. به شما می‌گویند فلان کس را دستگیر کردیم و در بازداشتگاه صدای جیغ و فریاد شخصی با صدای شبیه او را برایتان پخش می‌کنند.

۱۴. ممکن است با پیش‌کشیدن بحث‌های روابط جنسی شما و خانوادتان، شما را تحت فشار بگذارند. فریب این ترفند را نخورید.

۱۵. اگر در دوران بازجویی شکستید و تسلیم خواست بازجو شدید، حتما در بازپرسی و دادیاری به طور مکتوب برای بازپرس و دادیار پرونده بنویسید که تحت فشار بازجو مجبور به اعتراف اجباری شده‌اید و آن اعترافات تحت فشار بوده است. تاکید می‌کنیم که همه چیز را مکتوب کنید. حتی اگر بازپرس یا دادیار به پاسخ شما اعتراض کرد نیز کوتاه نیاید. چند سالی می‌شود که دیگر جلوی بازپرس و دادیار کسی را شکنجه نمی‌کنند. ممکن است که تهدید شوید، ولی نترسید و محکم سر حرف‌تان بایستید. حتی اگر تهدید به طولانی‌ترشدن بازداشت موقت شدید، کوتاه نیایید. در جواب تمام سوالات بازپرس و دادیار موارد شکنجه و فشار را بنویسید و از انجام این کار نترسید. در تمامی اوراق به فشارها به صورت مفصل اشاره کنید. فرض کنید بقیه ورق‌های بازجویی قرار است از پرونده برداشته شود. پس در تمام برگه‌های بازپرسی به اعمال فشار جسمی و روحی اشاره کنید. اگر این کار را بکنید، در بازداشتگاه فشار بر شما حتما کمتر می‌شود. این را مطمئن باشید.

۱۶. هر چقدر در مقابل بازجو و بازپرس بیش‌تر حالت تسلیم بگیرید، فشار بر شما بیش‌تر می‌شود و پرونده شما سنگین‌تر.

۱۷. در بازداشتگاه هر روز به خودتان یادآوری کنید که بازجوها و بازپرس بزرگ‌ترین دشمن شما هستند، وظیفه آن‌ها این است که با انواع روش‌ها، تهدیدها، وعده‌های دروغ سعی در سنگین‌تر کردن پرونده شما دارند. فریب مهربان شدن‌شان را نخورید و نیز از تهدیدهای آن‌ها نترسید. بازجویی که ترس شما را ببیند، فشار بر شما را بیش‌تر می‌کند. تاکید می‌کنیم که هدف اصلی بازجو ترساندن شما ست. اگر ترسیدید یا ترس‌تان را نشان دادید، او برنده شده. اگر نه، برنده شمایید.

۱۸. در جواب‌دادن به هر سوال، فکر کنید. ببینید جواب به هر سوال کدام یک از موارد قانونی که اشاره کردیم را می‌تواند شامل می‌شود. مثلا اگر اعتراف کنید یک مطلب انتقادی در جایی به‌تنهایی نوشته‌اید، می‌تواند تبلیغ علیه نظام ماده ۵۰۰ در نظر گرفته شود با حداکثر یک سال حکم حبس. یا نشر اکاذیب و تشویش اذهان عمومی حداکثر ۲ سال. ولی اگر اعتراف کنید که با دوست‌تان تصمیم گرفتید فلان کار را بکنید یا با دوست‌تان به تظاهرات رفته‌اید، می‌شود اجتماع و تبانی در ماده ۶۱۱ و حداکثر ۵ سال حکم.

۱۹. بازجو از شما می‌خواهد تک‌نویسی کنید و به شما می‌گوید این به نفع شما ست در حالی که این کار بیش‌تر از همه به ضرر خود شما ست. با تک‌نویسی علیه دوستان یا دیگران، در اصل دارید دایره اختیار بازجو برای گسترده‌ترشدن اتهامات علیه خودتان را فراهم می‌کنید. به تفاوت مجازات ماده ۵۰۰ و ۶۱۱، تبلیغ علیه نظام و اجتماع و تبانی توجه کنید. تفاوت ۴ سال حبس است، شما با تک‌نویسی برای دوست‌تان، حکم خودتان را هم ۴ سال افزایش می‌دهید!

۲۰. اگر اعتراف کنید که با دوستم یک گروه درست کرده‌ایم، می‌توانند به شما اتهام تشکیل گروه بزنند با ده سال حکم.

۲۱. بسیار مهم است که چه طور به سوالات جواب دهید و چه ضمیری یا چه فعلی در پاسخ‌تان به کار ببرید.

۲۲. واردکردن شوک روانی، دادزدن بر سر شما، توهین، ایجاد صداهای وحشتناک، پخش نوحه و عزا در سلول برای به‌هم‌ریختن اعصاب شما، قطع هواخوری، زدن چشم‌بند، اجازه نشستن ندادن برای ساعات متوالی، اجازه تماس ندادن با خانواده برای روزها و هفته‌ها، عدم اجازه استفاده از دستشویی، تهدید به تجاوز جنسی خود شما یا

خانواده‌تان، تهدید به دستگیری عزیزان‌تان، خبر جعلی دستگیری عزیزان‌تان، تهدید به قتل شما یا عزیزان‌تان، تهدید به گرفتن مجازات سنگین در دادگاه در صورت عدم همکاری، تهدید به انفرادی طولانی‌مدت و تهدید به آسیب‌زدن به خانواده، از روش‌های معمولی بازجوها ست.

۲۳. در برخی موارد حتی ضرب‌وشتم، ریختن آب سرد، برهنه‌کردن، اجازه‌ندادن برای خوابیدن به مدت طولانی و در مواردی اجرای اعدام نمایشی از دیگر شیوه‌های شکنجه فیزیکی است

۲۴. بازجو در صورت عدم همکاری شما ممکن است مدتی شما را در انفرادی رها کند و چندین روز بازجویی نداشته باشید. از طولانی‌شدن دوران بازداشت نترسید. سخت است ولی به این فکر کنید که در صورت تسلیم‌شدن بر بازجو، احتمالا چند سالی را در زندان سپری خواهید کرد.

۲۵. طبق قانون، ضابط قضایی باید بعد از بررسی مدارک جرم و اثبات وقوع جرم از سیستم دادستانی و بازپرس و دادیار حکم بازداشت شما را بگیرد و شما را با اتهام‌های مشخص تفهیم اتهام کند و شما فقط و فقط موظفید در خصوص آن اتهامات در بازجویی پاسخگو باشید. هر جا سوالی خارج از بحث تفهیم اتهام از شما شد، در پاسخ، به صورت کتبی بنویسید که این سوال مربوط به اتهامات اینجانب نیست و به آن پاسخ ندهید. چون هر پاسخی می‌تواند اتهام جدیدی برای شما باشد.

۲۶. می‌شود به روند بازجویی به شکل یک مسابقه نگاه کنید، یک طرف شمایید و طرف دیگر سیستم قضایی، هرگونه کوتاه‌آمدن در این مسابقه، می‌تواند برایتان سال‌های سال دوری از خانواده را در پی داشته باشد.

۲۷. در بازداشتگاه برای خودتان سرگرمی‌های فکری درست کنید.

۲۸. در هر موردی و هر پاسخی خیلی خوب به سوال و پاسخی که می‌خواهید بنویسید، فکر کنید. پاسختان را خیلی کوتاه و بدون شرح و بسط بنویسید. خودتان را جای بازجو بگذارید و ببینید با خواندن پاسخ شما چطور می‌تواند از این پاسخ علیه خودتان استفاده کند.

۲۹. اگر فشار روی شما خیلی زیاد شد، گاهی بد نیست برای کاهش فشار نقش کسی را بازی کنید که خود را باخته است، ولی مراقب باشید اطلاعاتی ندهید که علیه

خودتان استفاده شود.

۳۰. همواره اصرار کنید به مشخص‌شدن موارد اتهامی و اگر موارد اتهامی در یک سوال، با موارد تفهیم اتهام بازپرسی یکسان نبود، به آن اعتراض کنید و پاسخی ندید.

۳۱. خودتان را به هیچ چیزی حساس نشان ندید. مثلا من به سیگار حساسیت دارم و دود سیگار اذیتم می‌کند. یا اگر گفتند فلان عزیزت را دستگیر می‌کنیم و وحشت شما را از این تهدید ببینند، امکان دستگیری آن عزیزتان را بیش‌تر کرده‌اید، انعکاس رفتار شما باید مثل این باشد که خب دستگیر کنید، ایشان که کاری نکرده!! در کل نقاط ضعفتان را مخفی کنید.

۳۲. اطلاعات‌تان را در مغزتان طبقه‌بندی کنید و با خودتان قرار بگذارید که هدف‌تان ندادن اطلاعات است، ولی اگر در فشار حداکثری مجبور به افشای اطلاعات شدید، مقدار اطلاعاتی که نمی‌تواند منجر به صدور حکمی علیه شما شود را به بازجو بدهید.

۳۳. اگر در حین بازجویی، چنانچه مجبور به اعتراف شدید، سعی کنید موضوع را بیش‌تر حول فعالیت‌های خودتان نگه دارید و در اعترافات خود، از درگیرکردن دیگر فعالان تا حد امکان خودداری کنید.

۳۴. هر کجا هر چیزی را که ممکن بود، تکذیب کنید: مثلا بگویید «من آن‌جا نبودم»، «فلانی را نمی‌شناسم»، «با او تماسی نداشته‌ام»، «من در فلان مکان فقط رهگذر بودم» و پاسخ‌های از این دست.

۳۵. از برملاشدن دروغ نترسید، گاهی حرف راست هزینه‌های سنگینی برایتان خواهد داشت.

۳۶. سعی کنید نشکنید ولی اگر در بازجویی شکستید، یادتان نرود که پایان دنیا نیست، سعی کنید حداقل اطلاعات را بدهید و حتما همان را در جلسه بازپرسی یا دادیاری تکذیب کنید و مکتوب بنویسید که تحت شکنجه جسمی، روحی بوده و با القای بازجو آن‌ها را نوشته‌اید و حتما این را در بازپرسی در تمامی صفحاتی که بازپرس جلوی شما می‌گذارد، به شکل مشروح ذکر کنید.

۳۷. گاهی برای شما جلسات مواجهه حضوری با دوستان‌تان ترتیب می‌دهند. یعنی دوستانی را که آن‌ها را هم دستگیر کرده‌اند را روبروی شما قرار می‌دهند و آن‌ها ممکن است حرف‌هایی علیه شما بزنند، درکش کنید و ناراحت و عصبانی نشوید،

ولی از موضع خودتان کوتاه نیایید و علیه او هم حرفی نزنید و جلوی بازپرس بگویید دوست‌تان احتمالا تحت فشار و با القای بازجوها آن مطالب را عنوان کرده یا در شرایط روحی طبیعی نبوده که چنین چیزی می‌گوید.

۳۸. اگر مورد ضرب‌وشتم قرار گرفتید، واکنش‌تان به حس درد، بیش‌تر از حد واقعی باشد. اگر بازجو حس کند شما به اندازه کافی درد نمی‌کشید ضرب‌وشتم را شدیدتر می‌کند و محکم‌تر شما را می‌زند، اگر شدید کتک خوردید، خیلی سریع واکنش رعشه یا بی‌هوشی به خودتان بگیرید. به خودتان بگویید، کسی که برای گرفتن اطلاعات مجبور به اعمال فشار فیزیکی می‌شود در نقطه ضعف است نه شما! به همین شکل به خودتان روحیه دهید.

۳۹. هر زمانی که کتک خوردید، پس از بازگشت به سلول از نگهبان بند درخواست قلم و کاغذ کنید و کتک‌خوردن را به مسئول بند گزارش کنید. شاید بازجو از این کار شما عصبانی شود، ولی مطمئن باشید به نفع شما ست و در بیشتر اوقات باعث می‌شود شکنجه قطع شود. اگر به شما قلم و کاغذ ندادند، این موضوع را شفاهی به مسئول بند مورد نظر گزارش کنید و درخواست کنید شما را به بهداری ببرند و اگر بردند به دکتر هر اتفاقی که افتاده را بگوید. دکتر موظف به ضبط اظهارات شما ست. از دکتر معاینه پزشک قانونی درخواست کنید مخصوصا زمانی که اثر ضرب‌وشتم در تن شما مشخص باشد.

۴۰. در صورت شکستن در بازجویی، خیلی گنگ پاسخ‌ها را بنویسید و سعی کنید خیلی بدخط و غیر قابل خواندن و غیر از دست‌خط خودتان باشد و همان‌طور که بارها گفتیم، در حضور بازپرس آن مطب را رد کنید و از همین بدخط‌بودن به عنوان یک دلیل اعتراف تحت شکنجه، استفاده کنید.

۴۱. بازجو ممکن است از بعضی پاسخ‌های شما خوشش نیاد و چندین بار پاسخ شما را پاره کند و سوال جدید بپرسد، شما کوتاه نیاید و کار خودتان را بکنید.

۴۲. به سوالات شفاهی، کتبی جواب بدید و هرگز نوشته‌های بازجو یا بازپرس را امضا نکنید

۴۳. حاضر به اجرای سناریوی اعتراف جلو دوربین نشوید، از همین علیه شما استفاده می‌کنند. اگر تحت شکنجه مجبور به پذیرش شدید، سعی کنید نامفهوم صحبت

کنید و مشخص باشد که اعترافتان به‌زور بوده است.

۴۴. گاهی بازجو به شما می‌گوید که در صورت نوشتن درخواست عفو و توبه، برایتان عفو می‌گیرد و آزاد می‌شوید، در این تله نیوفتید زیرا عفو برای کسی است که حکم قطعی دارد. فراموش نکنید که در روند بازجویی هیچ کس مشمول عفو نمی‌شود. درخواست عفو و توبه‌کردن، مدرکی است علیه شما که شما جرمی مرتکب شده‌اید که درخواست عفو کرده‌اید.

۴۵. دادسرا و دادگاه در بیان نوع سوالات خود با محدودیت‌هایی قانونی روبرو هستند و متهم می‌تواند از پاسخگویی به سوالات غیرقانونی آن‌ها خودداری کند. در اکثر موارد متهمان سیاسی مجبور به پاسخگویی به سوالات می‌شوند. بهتر است برای آن که بعدها بتوانید فشار حاکم بر ایام بازجویی را اثبات کنید، در پاسخ به هر یک از این سوالات به طور کتبی، اول به غیرقانونی‌بودن سوال اشاره کنید و سپس پاسخ خود را بنویسند. در ادامه نمونه سوالاتی که غیر قانونی محسوب می‌شوند و متهم می‌تواند از پاسخگویی به آن‌ها خودداری کند را ببینید.

یک- بازجو، بازپرس یا قاضی نمی‌تواند سوالاتی که ارتباطی با جرم یا جرائم تفهیم‌شده به متهم ندارد را از او بپرسد. به عنوان مثال اگر جرم تفهیم‌شده به موکل، «اخلال در نظم عمومی از طریق حضور در تظاهرات خیابانی» است، نمی‌تواند در مورد «شرب خمر» یا «مصرف مواد مخدر» یا «رابطه نامشروع» سوال کنند. مگر آن که مثلا اتهام شرب خمر قانونا به متهم تفهیم شود که در این صورت هم مرجع رسیدگی به آن نمی‌تواند دادگاه انقلاب باشد.

دو- سوال‌کردن درباره عقاید متهم با توجه به این‌که در قانون اساسی تفتیش عقاید ممنوع است، نمی‌توان از متهم در مورد اعتقادات و نظراتش سوال کرد و شما مجازید پاسخی با این سوالات ندهید. به عنوان مثال نمی‌توان از او پرسید نظرش در مورد حوادث پس از انتخابات چه بوده یا او چه نظری در مورد رهبر یا دیگر مسئولان حکومتی دارد. سوال در مورد اعتقادات مذهبی فرد و انجام اعمال عبادی چون نمازخواندن و امثال آن نیز تفتیش عقیده محسوب می‌شود.

سه- معمولا سوال‌کردن در مورد امور خصوصی متهم و اطرافیان، صرفا به عنوان روشی برای آزار روانی متهم به کار می‌رود. پیشنهاد می‌شود از هرگونه پاسخگویی

به این سوالات خودداری کنید. سوال در خصوص روابط خانوادگی، عاطفی و جنسی متهم یا دیگران از جمله این موارد است.

چهار- سوالات تلقینی: قاضی نمی‌تواند در سئوال خود به نحوی ارتکاب جرم را به متهم القا کند. مثلا نمی‌تواند در حالی که اتهام شخص اخلال در نظم عمومی از طریق شرکت در تظاهرات است و متهم آن را انکار می‌کند از او بپرسد که چه کسان دیگری را برای اعتراض با خود بردی؟

پنج- اغفال متهم: فریب‌دادن متهم برای وادارکردن متهم به پاسخگویی و این که علیه خود یا دیگری اقرار کند، از موارد غیر قانونی است.

شش- روش شایع آن است که به متهم گفته می‌شود چنانچه برخی اقدامات یا اتهامات را قبول کند، می‌توانند به او تخفیف دهند یا او را آزاد کنند. ولی در عمل، همین اعترافات است که به عنوان مدرک جرم در دادگاه به کار می‌رود و امکان دفاع از متهم در مرحله دادگاه را تا حد زیادی محدود می‌کند. بازجویان به برخی از فعالان سیاسی سال‌های اخیر که اعدام شده‌اند، گفته بودند اگر در پرونده، دادگاه یا در مقابل دوربین، اتهامات منتسب‌شده را بپذیرند، آزاد می‌شوند یا با حکم حبس کم‌تری روبرو خواهند شد. در نهایت حکم اعدام علیه آن‌ها بر اساس همین اعترافات صادر شده بود.

هفت- تک‌نویسی در پرونده‌های سیاسی برای جمع‌آوری مدرک علیه دیگر فعالان سیاسی و اجتماعی: در این روش از متهم می‌خواهند کلیه اطلاعات خود را در مورد شخص یا اشخاص مختلف بیان کند. این سئوال غیر قانونی است و متهم می‌تواند به آن پاسخ ندهد. در صورتی که متهم مجبور به نوشتن می‌شود، بهتر است تا جای ممکن هر گونه آشنایی انکار شود و در صورتی که این امکان وجود نداشت، به ارائه اطلاعات بسیار کلی بسنده کند. باید بسیار دقت شود که از هر گونه ارائه اطلاعات در مورد عادات شخصی، روابط خصوصی و همچنین فعالیت‌های اشخاص که می‌تواند منجر به شناخت بیش‌تر از آن‌ها شود، خودداری کرد. برخی از بازداشت‌شدگان فکر می‌کنند نوشتن اطلاعات عمومی به‌خصوص اطلاعاتی که قبلا منتشر شده، درباره کسانی که از آن‌ها خواسته می‌شود، بی‌ضرر خواهد بود. در حالی که ما هیچ گاه نمی‌دانیم اطلاعاتی را که در تک‌نویسی‌ها ارائه می‌کنیم، در پازل ماموران اطلاعاتی

چگونه استفاده خواهد شد. در کل تک‌نویسی درباره یک نفر نه تنها برای دیگران مشکل ایجاد می‌کند بلکه پرونده شما را هم سنگین‌تر می‌کند چون شما اعتراف می‌کنید از امری که از نظر قاضی جرم محسوب می‌شود، مطلع بوده‌اید.

هشت- سوال در مورد رمزهای مربوط به ارتباطات شخصی متهم چون ایمیل، فیس‌بوک، وبلاگ و شبکه‌های اجتماعی دیگر: کشف دلایل جرم، وظیفه کسی است که مدعی وقوع جرم و منتسب‌بودن آن به متهم است، بنابراین متهم هیچ وظیفه‌ای ندارد تا با دراختیارگذاردن لیست مکالمات خصوصی خود، آن‌ها را در پیداکردن دلیل یاری کند. این سوال و درخواست از طرف بازجو و مقامات تحقیق غیرقانونی است و متهم می‌تواند از پاسخگویی به آن خودداری کند. با توجه به اجبار متهمان سیاسی به ارائه پسورد، پیشنهاد می‌شود پس از بازداشت متهم، بلافاصله پسورد ایمیل یا دیگر ارتباطات اینترنتی او توسط نزدیکان تغییر داده شود. همچنین متهم می‌تواند پسورد ایمیل‌هایی را به آن‌ها بدهد که محتوای آن‌ها نمی‌تواند هیچ‌گونه اتهامی را علیه او یا دیگری ثابت کند.

۱۵ استراتژی برای حبس‌کشی و وقت‌گذرانی در انفرادی

با وجودی که تحمل زندان انفرادی بسیار دشوار است، اما روش‌هایی مشخص و اثبات‌شده‌ای برای مقابله با آن وجود دارد. در ادامه به بررسی ۱۵ روش از موثرترین راهکارهای کاهش فشارهای ناشی از زندان انفرادی را بررسی می‌کنیم:

۱. برنامه‌ریزی روزانه و ساعت‌بندی ورزش یا رقص روزانه در سلول به گونه‌ای که ضربان قلب‌تان بالا برود و عرق کنید.
۲. خوردن صبحانه و غذای مرتب و نوشیدن آب.
۳. فکرکردن به خاطرات خوب و پناه‌بردن به قوه تخیل و خاطره‌سازی.
۴. تماس با افراد در سلول‌های کناری در صورت امکان، بدون صحبت در مورد مسائل حساس.
۵. انجام مدیتیشن ساده مثلا در حد ۴ ثانیه دم و ۴ ثانیه بازدم.
۶. تمیزکردن سلول.
۷. درست‌کردن بازی‌های یک‌نفره مثل «سودوکو» یا هر بازی شبیه به آن.

۸. فکرکردن به این موضوع که تمام این اتفاق‌ها روزی تبدیل به خاطره خواهد شد.
حمام و دستشویی رفتن مرتب.
۹. خواندن دیوارنوشته‌ها و نوشتن اسم و مطالبی برای زندانیان بعدی در صورت امکان.
۱۰. مرور ذهنی فیلم‌ها و کتاب‌هایی که قبلا دیده یا خوانده‌اید و تغییر سناریوهای آن‌ها.
۱۱. ترانه‌خواندن حتی اگر شده به صورت زمزمه.
۱۲. سعی کنید فکر خود را از مشکلات خانواده و عزیزان‌تان منحرف کنید.
۱۳. هر روز درخواست روزنامه، کتاب و تماس با خانواده داشته باشید حتی اگر هر روز با این درخواست‌ها مخالفت شود، باز تکرار کنید.
۱۴. استفاده از هر موقعیت هواخوری حتی اگر با چشم‌بند باشد و در هر شرایط آب و هوایی بد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- آیا به رفتار و وعده بازجو می‌توان اطمینان کرد؟

الف) بله، اگر خوش‌برخورد و محترم باشد.

ب) بله، اگر بگوید که با موارد غیرقانونی و نقض حقوق مخالف است.

ج) خیر، اگر نگوید که حتما زمینه آزادی را فراهم می‌کند.

د) خیر، در هیچ شرایطی نباید اعتماد کرد.

۲- در صورت فشار برای «اعتراف علیه خود» از سوی بازجو/بازپرس ...

الف) با بررسی شرایط و وعده آن‌ها می‌توانم تصمیم بگیرم که اعتراف تلویزیون را انجام دهم یا نه.

ب) در صورت محقق‌شدن خواسته‌هایم (مثل ملاقات با خانواده)، تن به اعتراف اجباری می‌دهم.

ج) تا حد امکان زیر بار اعتراف علیه خود نروید.

د) بسته به شرایط تصمیم می‌گیرم.

۳- در دوران بازجویی، اگر بازجو خواست که زندانی درخواست «عفو و توبه» کند ...

الف) زندانی می‌تواند بپذیرد به شرط این‌که بازجو قول آزادی بدهد.

ب) زندانی نباید بپذیرد. عفو برای کسی است که حکم قطعی دارد، در روند بازجویی کسی مشمول عفو نمی‌شود.

ج) زندانی می‌تواند بپذیرد. به شرط این‌که دادیار نیز آن‌جا حضور داشته باشد.

د) زندانی نباید بپذیرد. چون عفو باید فقط از طرف رییس قوه قضائیه پیشنهاد داده شود.

درس نه
اعتراضات، ۴: استراتژی شرکت در تظاهرات

تظاهرات و تجمعات اعتراضی در نظام جمهوری اسلامی همواره با خطراتی همراه هستند که شناخت و ارزیابی آن‌ها امری حیاتی است. این خطرات می‌توانند از سرکوب فیزیکی گرفته تا مشکلات امنیتی و حتی ازدست‌دادن جان افراد باشد.

به منظور مقابله با این خطرات و آمادگی برای مواجهه با آن‌ها، لازم است قبل از شرکت در هر تجمع اعتراضی، برنامه‌ریزی کنیم و آگاهانه و آماده در تظاهرات حاضر شویم. اهمیت توجه به این امور و انجام اقدامات مناسب در این زمینه به منظور جلوگیری از وقوع حوادث ناخوشایند و حفظ سلامت و امنیت افراد بسیار ارزشمند است. در ادامه ۱۱ استراتژی مهم برای شرکت در تظاهرات را بررسی می‌کنیم.

۱۱ استراتژی مهم برای شرکت در تظاهرات

۱. شناسایی و ارزیابی خطرات

تشخیص و ارزیابی دقیق خطرات مربوط به تظاهرات اعتراضی، از جمله اولویت‌های اصلی است. این ارزیابی باید شامل تحلیل امنیتی و تهدیدات محتمل و شامل اقدامات سرکوبی نیروهای امنیتی باشد. قبل از شرکت در هر تجمع یا تظاهرات، ارزیابی دقیقی از خطرات مربوطه، بسیار ضروری است.

باید به‌دقت مسائل امنیتی و تهدیدات محتمل را به‌درستی بررسی کنیم و آمادگی روحی و جسمی خود را ارزیابی کنیم. با توجه به تجاربی که از اعتراض‌های سال‌های اخیر کسب کرده‌ایم، می‌دانیم که احتمال وقوع سرکوب و وقایع ناخوشایند در هر نوع تظاهرات و تجمع وجود دارد. پس برای حضور در هر تظاهرات یا تجمع، باید آمادگی و هوشیاری کامل و آگاهی از امکان روبروشدن با مشکلات را داشته باشیم.

باید بپذیریم که ممکن است با واقعیت‌های ناخوشایندی روبرو شویم، اما باید در هر شرایطی روحیه خود را حفظ کرده و با هوش و احتیاط عمل کنیم.

۲. اطلاع‌رسانی و آموزش به خانواده و افراد نزدیک به خود

این امر بسیار حیاتی است و با توجه به سوابق نیروهای سرکوبگر رژیم در ناپدیدسازی قهری بسیاری از فعالان سیاسی، مدنی و دانشجویی در سال‌های اخیر، بهتر است قبل از شرکت در تظاهرات به دوستان نزدیک و خانواده اطلاع دهیم تا آن‌ها نیز برای هرگونه وضعیت آماده باشند.

مواردی مانند مخفی‌کردن هرگونه مدارک فیزیکی یا الکترونیکی که ممکن است برای شما مشکل ایجاد کنند و آموزش نحوه انجام این اقدامات در صورت دستگیری به آن‌ها بسیار حیاتی است. همچنین، آموزش‌دادن به نزدیکان درباره ارتباط با رسانه‌های آزاد پس از دستگیری شما، از جمله موارد بسیار مهم است. تجربه نشان داده است که بهترین استراتژی خانواده پس از دستگیری فعالان سیاسی و مدنی، اطلاع‌رسانی به رسانه‌ها و پیگیری روزانه در دادسرای مربوطه است.

از آنجا که نیروهای امنیتی همواره دنبال قربانیانی می‌گردند که صدایی ندارند، بنابراین آن‌ها گاهی خانواده را تهدید می‌کنند که اگر موضوع پرونده شما را به رسانه‌ها اعلام کنند، پرونده شما سنگین‌تر خواهد شد، اما این موضوع به هیچ وجه صحیح نیست. بنابراین خانواده‌ها نباید به این ادعاهای آن‌ها اعتماد کنند. سکوت خانواده امکان شکنجه‌شدن شما و وادارکردن‌تان به قبول اعتراف اجباری، طبق سناریوهای نیروهای امنیتی را به‌شدت زیاد می‌کند.

۳. بررسی جغرافیایی کامل منطقه

بررسی جغرافیایی شامل بررسی دقیق و جامع از جنبه‌های مختلف است که می‌تواند در

زمان تظاهرات و تجمعات اعتراضی بسیار مفید باشد. در ادامه برخی از این جنبه‌ها را مرور کنیم.

الف- شناسایی نقاط امن

بررسی جغرافیایی منطقه به منظور شناسایی مکان‌هایی که از نظر امنیتی مطمئن‌تر هستند، اهمیت زیادی دارد. این شامل شناسایی محل‌هایی است که دور از مرکز تظاهرات و تجمعات هستند یا دارای فضای مناسبی برای پنهان‌شدن و فرار در صورت هر گونه اتفاق ناگوارند.

ب- شناسایی راه‌های فرار

شناسایی مسیرهای ممکن برای فرار در صورت بروز خطرات از جمله اقدامات حیاتی است. این شامل بررسی مسیرهای جایگزین، خیابان‌های کوچک، فرعی، پیاده‌روها و همچنین ایجاد یک برنامه فرار مطمئن است.

پ- شناسایی و پیش‌بینی مکان‌های مورد حمله سرکوبگران

بررسی دقیق جغرافیایی منطقه شامل شناسایی و پیش‌بینی مکان‌هایی که به عنوان هدف حمله نیروهای سرکوب ممکن است انتخاب شوند، بسیار مهم است. در کل، بررسی جغرافیایی کامل منطقه قبل از شرکت در تظاهرات و تجمعات می‌تواند به شما کمک کند تا برای مواجهه با خطرات و حفظ امنیت خود و دیگران، بهترین تصمیمات را بگیرید.

۴. آشنایی با روش‌های پوشاندن صورت

برای مخفی‌ماندن و حفظ هویت، آشنایی با روش‌های مختلف پوشاندن صورت از جمله اقدامات مهمی است که تظاهرکنندگان باید به آن‌ها توجه کنند. استفاده از ماسک و عینک دودی، کلاه لبه‌دار و به همراه‌داشتن یک دست لباس با رنگی متفاوت در یک کوله‌پشتی کوچک می‌تواند بسیار موثر باشد.

۵. تشکیل گروه‌های مقاومت در برابر نیروهای سرکوب و حمایت از دیگر تظاهرکنندگان

تجربه‌های اخیر نشان می‌دهد که در تجمعات و تظاهرات‌ها امکان دستگیری کسانی که از

بقیه جمعیت معترضان فاصله می‌گیرند، بیش‌تر است. لذا در زمان حضور نیروی سرکوب، یکی از بهترین استراتژی‌ها به‌هم‌پیوستن هرچه بیش‌تر جمعیت است.

دقت کنید که نیروی سرکوب نیز ابتدا تلاش می‌کند یک تجمع را چندتکه کنند و سپس دست به بازداشت می‌زنند. اگر یک نیروی سرکوب انتظامی یا لباس‌شخصی سعی در دستگیر یکی از تظاهرکنندگان کرد، به کمک او بروید. شما با ایجاد جمعیت و حرکت به سمت نیروی سرکوب می‌توانید آن‌ها را گیج و سردرگم کنید.

۶. همکاری با سایر گروه‌ها و افراد

همکاری با سایر گروه‌ها و افراد معترض در تظاهرات و تجمعات می‌تواند قدرت و اعتبار شما را افزایش دهد. ایجاد شبکه‌های حمایتی و همکاری در مواجهه با نیروهای سرکوب می‌تواند به شما کمک کند تا با خطرات کمتری روبرو شوید.

۷. ارتباط با رسانه‌ها و سازمان‌های بین‌المللی

اطلاع‌رسانی به رسانه‌ها و سازمان‌های بین‌المللی در صورت بروز حوادث و خطرات حین اعتراضات می‌تواند به حفظ امنیت شما و دیگر معترضان کمک کند و فشار بر رژیم افزایش یابد.

۸. مقابله با گاز اشک‌آور و اسپری فلفل

نیروی‌های سرکوب برای متفرق‌کردن جمعیت یا چندپاره‌کردن آن، اغلب از انواع گازهای اشک‌آور و اسپری‌های فلفل استفاده می‌کنند. در درس دهم به روش‌های مواجهه و مقابله با گاز اشک آور می‌پردازیم.

۹. پرهیز از خشونت

نیروی سرکوب رژیم همواره سعی می‌کند یک تظاهرات مسالمت‌آمیز را به خشونت بکشاند. از آنجایی که نیروی سرکوب جمهوری اسلامی به سلاح گرم و سیستم دفاعی و نیروهای آموزش‌دیده مجهز است، مسلما در صورت بروز خشونت، برنده خواهد بود. بنابراین تا حد امکان از خشونت پرهیز کنید و دیگران را نیز به عدم خشونت دعوت کنید.

به این نکته توجه کنید که اکثر انقلاب‌ها و جنبش‌های پیروز در دهه‌های اخیر، زمانی به پیروز ملت ختم شد که نیروی سرکوب و نظامی نسبت از دستور سرکوب سرپیچی کرده و به ملت پیوسته‌اند. نیروی نظامی و سرکوب در صورتی به مردم می‌پیوندد که تظاهرات مسالمت‌آمیز باشد.

۱۰. ترک محل، در صورت استفاده نیروهای سرکوبگر از سلاح جنگی

اگر نیروی سرکوب مانند اعتراضات آبان ۹۸ و وقایع جنبش مهسا در سال ۱۴۰۱ از گلوله‌های سرکوب و جنگی استفاده کرد، که عملی جنایتکارانه است، هر چه سریع‌تر محیط را ترک کنید.

۱۱. کمک به افراد زخمی

در حد امکان سعی کنید زخمی‌ها را از محل درگیری و شلوغی دور کنید.

۱۲ ابزار لازم برای شرکت در تظاهرات

۱. **کوله‌پشتی کوچک:** هر شرکت‌کننده‌ای در تظاهرات باید احتمال این را بدهد که ممکن است در حین تظاهرات برای فرار از دست نیروی سرکوب و رسیدن به مکان امن، نیاز به دویدن داشته باشد. حمل کیف روی‌دوشی یا کیف دستی در این حالت می‌تواند برایتان دردسرساز باشد. پس کوله‌پشتی بردارید.
۲. **کفش راحتی:** کفش راحت به پا کنید به طوری که بتوانید با آن بدوید. از پوشیدن کفش‌های فنسی، پاشنه‌بلند و ناراحت اجتناب کنید، کفش‌های ورزشی مخصوص پیاده‌روی و دویدن بهترین گزینه است برای این کار.
۳. **شلوار مناسب و راحت**
۴. **بلوز راحت آستین‌دار**: این مسئله هم برای جلوگیری از آسیب در اثر گاز اشک‌آور و هم شناسایی‌نشدن آثار ویژه مانند خالکوبی دست و بازو بسیار مهم است.
۵. **چفیه، شال و کلاه:** به‌همراه‌داشتن این‌ها برای پوشاندن سر و صورت، در صورت مواجهه با گاز اشک‌آور خیلی می‌تواند مفید و کمک‌کننده باشد.
۶. **عینک اسکی یا شنا:** به‌همراه‌داشتن این نوع از عینک‌ها برای مواجهه با گاز

اشک‌آور و اسپری فلفل مفید است.

۷. **عینک آفتابی و کلاه لبه‌دار و ماسک:** به‌همراه‌داشتن آن‌ها برای جلوگیری از شناسایی توسط فیلم برداری‌های ماموران سرکوب ضروری است.

۸. **یک پیراهن اضافی:** به‌همراه‌داشتن یک پیراهن اضافی در کوله‌پشتی، برای تعویض در صورت مواجهه مستقیم با گاز اشک‌آور یا هنگام فرار جهت عدم شناسایی می‌تواند نجات‌بخش باشد.

۹. **آب:** به‌همراه‌داشتن آب را فراموش نکنید. چه برای نوشیدن و چه برای شستن صورت، باید همیشه یک یا دو بطری آب تمیز در کوله‌پشتی خود داشته باشید. اگر می‌توانید، منابع آب تمیز را در محل تظاهرات در همان مراحل اولیه اعتراض یا تظاهرات شناسایی کنید تا اگر بطری آب‌تان خالی شد در اسرع وقت آن را دوباره پر کنید.

۱۰. **مقداری خوراکی ساده:** برای مواقع ضروری و جلوگیری از ضعف و افتادن فشار مقداری خوراکی به همراه داشته باشید.

۱۱. **مقداری پول نقد:** در صورت دستگیرشدن یا حین فرار، داشتن مقداری پول نقد می‌تواند مفید باشد.

۱۲. **یک دستگاه تلفن ساده بی‌نام‌ونشان:** همان‌طور که در جلسات قبل هم گفتیم، اگر می‌خواهید تلفن همراه با خود ببرید، یک دستگاه تلفن بی‌نام و نشان داشته باشید که هیچ اپلیکیشنی با شماره تلفن و با اسم خودتان یا آی.دی با مشخصات واقعی شما در آن وجود نداشته باشد. نصب اپلیکیشن Bridgefy در صورتی که تعداد زیادی از افراد در تجمع، آن را در موبایل خود نصب کرده باشند، می‌تواند راهکار بسیار خوبی در پخش خبر و فایل و عکس در حین تظاهرات در صورت قطع کامل یا منطقه‌ای اینترنت باشد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- در صورت دستگیری بهترین استراتژی خانواده و نزدیکان چیست؟

الف) پیگیری فقط از طریق دادسرای مربوطه.

ب) مخفی‌نگه‌داشتن موضوع دستگیری تا زمان دادگاه با هدف کاهش حساسیت‌ها.

ج) رسانه‌ای‌کردن موضوع دستگیری، پیگیری روزانه از دادسرا برای برقراری تماس و ملاقات با فرد دستگیرشده و مشاوره با وکیل حقوق بشری.

د) اعتماد به بازپرس و دادیار پرونده و صبوری و عمل مطابق خواست و وعده‌های آن‌ها.

۲- پیش از شرکت در اعتراضات، باید منطقه و محل اعتراضات را کاملا بررسی کنیم. با هدف...

الف) شناسایی نقاط امن.

ب) شناسایی نقاط امن و راه‌های فرار.

ج) شناسایی و پیش‌بینی مکان‌های مورد حمله سرکوبگران.

د) همه موارد بالا.

۳- «هنگام شرکت در اعتراضات ضدحکومتی باید صورت خود را بپوشانیم.»

الف) بله، برای حفظ امنیت خود.

ب) خیر، چون در این صورت ترسو جلوه می‌کنیم.

ج) بله، برای ترساندن ماموران.

د) خیر، چون در این صورت نمی‌توانیم دوستان‌مان را راحت پیدا کنیم.

درس ده
اعتراضات، ۵: مواجهه با گاز اشک‌آور

نیروهای امنیتی و انتظامی در درگیری‌های خیابانی برای متفرق‌کردن معترضین از راه‌های مختلفی استفاده می‌کنند. یکی از این راه‌های متفرق‌کردن معترضین، استفاده از گاز اشک‌آور است که موجب عوارض و خطراتی برای سلامت افراد می‌شود. در حالی که عوامل اشک‌آور معمولا برای کنترل شورش توسط نیروهای مجری قانون و پرسنل نظامی استفاده می‌شوند، استفاده از آن‌ها در جنگ‌ها توسط معاهدات بین‌المللی مختلف ممنوع شده است.

در صورتی که خود یا دوستان‌تان مورد حمله گاز اشک‌آور و فلفل قرار گرفتید به این نکات توجه کنید:

الف- گاز اشک‌آور برخلاف نامش، در واقع یک پودر کریستالی است که به صورت اسپری یا توسط یک حامل انفجاری نارنجک‌مانندِ کوچک، پخش می‌شود. گاز اشک‌آور می‌تواند باعث صدماتی هم شود. بخش فعال گاز اشک‌آور، گیرنده خاصی در بدن را هدف قرار می‌دهد که عمدتا برای ارسال سیگنال‌های درد به سیستم عصبی عمل می‌کند. هنگامی که یک کپسول گاز اشک‌آور منفجر می‌شود، پودر آن به هوا پاشیده می‌شود و به سطوح مرطوب مانند چشمان، عرق روی پوست، چربی در موها، دهان و راه‌های هوایی و بزاق و

مخاط دهان و سطوح چرب می‌چسبد.

ب- وقتی در معرض گاز اشک‌آور قرار گرفتید، چشمان‌تان می‌سوزد، دیدتان تار می‌شود و اشک می‌ریزید و بی‌اختیار پلک می‌زنید. هر چه مدت طولانی‌تری در معرض گاز باشید، شرایط بدتر می‌شود. این پودر همچنین راه‌های تنفسی شما را تحریک کرده، تنفس را سخت می‌کند و باعث سفت‌شدن قفسه سینه می‌شود. شما به طور خودکار شروع به سرفه می‌کنید و بینی و دهان شما به ترتیب مقادیر زیادی مخاط و بزاق ترشح می‌کنند.

۶ نکته موثر درباره آمادگی قبل از قرارگرفتن در معرض گاز اشک‌آور

۱- از روسری، ماسک یا چفیه استفاده کنید

تنها راه کاملا موثر برای محافظت از خود در برابر گاز اشک‌آور استفاده از ماسک ضد گاز است، اما معمولا تهیه ماسک ضد گاز و حمل آن به این سادگی‌ها نیست. بهترین کار بعدی این است که بینی و دهان خود را با یک روسری یا چفیه بپوشانید، بهتر است روسری یا چفیه را با آب خیس کنید. این کار از ورود پودر به مجاری تنفسی جلوگیری می‌کند و به شما اجازه می‌دهد خوب نفس بکشید.

۲- سر خود را بپوشانید

اگر می‌توانید با یک شال یا روسری یا چفیه، هم، سرتان و هم بینی و دهان‌تان را بپوشانید و اگر شال و چفیه بزرگ ندارید، کلاه هم مکمل خوبی برای ماسک شما است. در هر صورت پوشاندن مجاری تنفسی اولویت دارد و پس از آن اطمینان حاصل کنید که تا حد ممکن قسمت‌های سر خود را بپوشانید و اگر موهای بلندی دارید، آن‌ها را با کش ببندید یا ببافید. این کار باعث می‌شود بعدا به‌راحتی از شر پودر خلاص شوید.

۳- از عینک محافظ چشم استفاده کنید

داشتن یک عینک اسکی یا شنا که می‌تواند از ورود هر گونه ذرات گاز اشک‌آور به چشم شما جلوگیری کند. اگر عینک اسکی و شنا ندارید، عینک آفتابی نیز می‌تواند مفید باشد، اگرچه ایده آل نیست. عینک‌های ساده فقط از شما در برابر ذرات که مستقیما به سمت شما می‌آیند محافظت می‌کند، اما داشتن عینک طبی یا آفتابی از هیچ بهتر است.

۴- تا حد امکان پوست خود را بپوشانید

این ممکن است در دماهای گرم‌تر مشکل‌ساز باشد، اما اگر مجبور هستید لباسی را برای

تظاهرات انتخاب کنید، اصل این است که آستین‌دار باشد و پارچه آن متراکم‌تر باشد. توجه داشته باشید که پودر گاز اشک‌آور به لباس شما می‌چسبد، بنابراین اگر در معرض آن قرار گرفتید، باید در اسرع وقت لباس خود را تعویض کنید.

۵- در تظاهرات آرایش نکنید

درست است که کنارگذاشتن ریمل و رژ لب برای برخی ممکن است سخت باشد اما آرایش‌کردن می‌تواند در مواجهه با گاز اشک‌آور برایتان دردسرساز شود. همان‌طور که گفته شد، علاوه بر این‌که پودر موجود در گاز اشک‌آور به مخاط و سایر مایعات بدن می‌چسبد، می‌تواند به سطوح روغنی مواد آرایشی نیز بچسبد.

۶- از لنزهای تماسی استفاده نکنید

تجربه مواجهه با گاز اشک‌آور برای کسانی که از لنزهای تماسی استفاده می‌کنند به مراتب وحشتناک تر از سایر افراد است.

۱۴ اقدام مهم در صورت مواجهه با گاز اشک‌آور

۱. فورا فرد را به مکان امن و غیر آلوده منتقل کنید.
۲. فراموش نکنید که افراد مسن، کم سن‌وسال و افراد دارای آسم، آسیب‌پذیری بیش‌تری نسبت به بقیه دارند، ولی قبل از کمک به دیگران، ابتدا سر و صورت خود را بپوشانید و سپس به کمک دیگران بروید.
۳. پودر داخل گاز اشک‌آور از هوا سنگین‌تر است، بنابراین غلظت آن در سطح زمین بسیار بیش‌تر از ارتفاع بالا ست. اگر کسی را دیدید که به زمین افتاده، سعی کنید بلندش کنید تا سرش در ارتفاع بالاتر قرار بگیرد.
۴. از به‌زور بازکردن پلک فرد آسیب‌دیده پرهیز کنید.
۵. با دستان تمیز لنز چشمی را خارج کنید.
۶. از دست‌زدن به پوست و صورت و مالیدن چشم‌هاپ رهیز کنید.
۷. با سرم شستشو یا آب تمیز چشم‌ها را بشویید به طوری که آب مستقیما به چشم شما بخورد، اما از ورود آب به بینی جلوگیری کنید. از آب‌های راکد یا حوضچه‌ها در محل استفاده نکنید. چراکه حوضچه‌های آب می‌توانند به‌راحتی با گاز اشک‌آور پس از انتشار در هوا، آلوده شوند.

۸. از برخورد آب با پیشانی هنگام شستشوی چشم‌ها پرهیز کنید تا مواد شیمیایی بیش‌تری به چشم‌ها وارد نشود.
۹. هنگام شستشوی چشم‌ها، مرتب پلک بزنید.
۱۰. از یک دستمال یا حوله برای جلوگیری از ریختن آب به شانه‌ها و بدن استفاده کنید.
۱۱. بعد از ۵ دقیقه شستشوی چشم، چشم‌ها را ببندید و تمام سر و گردن را با آب بشویید.
۱۲. دوباره چشم‌ها را ۱۵دقیقه در معرض آب جاری قرار دهید و بشویید تا درد و سوزش‌تان برطرف شود.
۱۳. پس از رسیدن به منزل توجه کنید که کفش و لباس‌های در معرض گاز را حتی‌الامکان در خارج از خانه از تن در بیاورید تا محیط خانه را آلوده نکنید.
۱۴. ۱به محض رسیدن به منزل، دوش بگیرید. دوش آب سرد می‌تواند تحریک‌پذیری پوست‌تان را کاهش دهد.

۴ نکته مهم در خاموش‌کردن کپسول‌های گاز اشک‌آور

۱۵. در کل ترک محل و دورشدن از کپسول گاز اشک‌آور بسیار امن‌تر است.
۱۶. اگر پوشش خوبی دارید و می‌خواهید کپسول گاز را به سمت نیروهای سرکوب یا سمت دیگری پرتاب کنید، به یاد داشته باشید که کپسول در آن لحظه بسیار داغ است و در صورت نداشتن دستکش ضخیم می‌تواند سوختگی شدید برایتان ایجاد کند.
۱۷. یکی از راهکارهای ازکارانداختن کپسول گاز اشک‌آور، برگرداندن یک سطل یا مخروط ترافیکی روی آن است. ولی برای انجام این کار هم مطمئن شوید که سر و صورت خود را به‌خوبی پوشانده‌اید.
۱۸. اگر توانستید سطل پر از آبی در محیط تهیه کنید یا اگر حوض و جوی آبی در محدوده هست، با انداختن کپسول در داخل آب می‌توانید آن را خاموش کنید و از پخش بیش‌تر پودر در محیط جلوگیری کنید.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- اگر در معرض گاز اشک‌آور قرار گرفتید، کدام کار را نباید انجام دهید؟

الف) با سرم شستشو یا آب سرد چشم‌ها را بشویید.
ب) در صورت استفاده از لنز چشمی، با دستان تمیز آن را خارج کنید.
ج) چشم‌ها را به‌زور باز کنید.
د) فوری از مکان آلوده به گاز دور شوید.

۲- کدام راهکار برای خاموش‌کردن گاز اشک‌آور نادرست است؟

الف) انداختن آن به جوی آب یا یک سطل آب.
ب) انداختن آن در کوله پشتی.
ج) برگرداندن یک سطل یا مخروط ترافیکی روی آن.
د) پرتاب آن به سمتی دیگر.

۴- اگر احتمال می‌دهید در تظاهرات از گاز اشک‌آور استفاده شود، کدام کار را نباید انجام دهید؟

الف) پوشاندن سر و صورت با روسری، ماسک یا چفیه.
ب) استفاده از عینک محافظ چشم مثل عینک شنا.
ج) آرایش‌کردن و استفاده از مواد آرایشی.
د) پوشیدن لباس آستین بلند.

پاسخ‌نامه

در این بخش پاسخ‌های پرسش‌های آزمون ارزیابی درس‌ها را مشاهده می‌کنید.

درس یک:
۱- ج / ۲- ب / ۳- د
درس دو:
۱- الف / ۲- ج / ۳- ج
درس سه:
۱- د / ۲- ب / ۳- ج
درس چهار:
۱- ج / ۲- ب / ۳- الف
درس پنج:
۱- الف / ۲- ب / ۳- ب
درس شش:
۱- ج / ۲- ج / ۳- ج
درس هفت:
۱- ب / ۲- ب / ۳-ج
درس هشت:
۱- د / ۲- ج / ۳- ب
درس نه:
۱- ج / ۲- د / ۳- الف
درس ده:
۱- ج / ۲- ب / ۳- ج