

مقدمه

قطع اینترنت به طور فزاینده‌ای به عنوان ابزاری برای سرکوب حکومت مورد استفاده قرار می‌گیرد، به‌ویژه در دوره‌های اعتراضات سیاسی مانند آنچه در ایران شاهد هستیم. موارد قطع اینترنت که از محدودیت‌های جزئی مانند مسدودسازی داده‌های تلفن همراه تا خاموشی کامل اینترنت متغیر هستند، چالش‌های قابل‌توجهی را برای بخش‌های مختلف جامعه ایجاد می‌کنند، از جمله اقلیت‌های قومی، فعالان مدنی، روزنامه‌نگاران و گروه‌های مذهبی. هر یک از این گروه‌ها در زمان قطع اینترنت با خطرات منحصربه‌فردی مواجه می‌شوند؛ از سرکوب حکومتی تا دسترسی محدود به ابزارهای ارتباطی امن.

این پروتکل برای پاسخ به این چالش‌ها تهیه شده و راهبردهای ویژه‌ای را برای حفظ ارتباطات امن در قبل، حین و بعد از قطع اینترنت ارائه می‌کند. در این سند، بر اهمیت استفاده از ابزارهای ارتباطی امن، آموزش امنیت دیجیتال و شبکه‌های جایگزین مانند سیستم‌های همتا به همتا (P2P) و فناوری‌های مایه‌ورهای تأکید شده است. با به‌کارگیری این استراتژی‌ها، گروه‌های در معرض آسیب می‌توانند اثرات منفی قطع اینترنت را کاهش داده و از ارتباطات خود در برابر نظارت دولتی محافظت کنند.

اگرچه نباید فراموش کرد که تمرکز باید بر افزایش سواد امنیت دیجیتال، توزیع ابزارهای امن و ایجاد شبکه‌های مقاوم ارتباطی باشد تا ارتباط امن بین گروه‌های مختلف جامعه مدنی و فعالان سیاسی با یکدیگر و نهادهای حقوق بشری و رسانه‌ها حتی در محدودترین شرایط نیز تضمین شود. در این سند، خوانندگان با گام‌های عملی و توصیه‌هایی برای حفظ ارتباطات امن در زمان قطع اینترنت آشنا می‌شوند؛ از راه‌اندازی ابزارهای رمزنگاری مانند GPG گرفته تا استفاده از شبکه‌های مش و ارتباطات مایه‌ورهای برای دسترسی به اینترنت. همچنین، راهنمایی‌هایی در مورد اقدامات پیشگیرانه، مانند تدوین برنامه‌های پشتیبان، آموزش‌های جامعه‌محور، آماده‌سازی پیش از قطع و بازیابی پس از قطع ارائه می‌شود که افراد و سازمان‌ها را قادر می‌سازد تا در برابر اختلالات اینترنتی، متصل و مقاوم بمانند.

قطع اینترنت به چه معناست؟

قطع اینترنت به معنای اختلال عمدی در اینترنت یا ارتباطات الکترونیکی است که توسط دولت‌ها یا نهادهای خصوصی برای کنترل جریان اطلاعات انجام می‌شود. قطع اینترنت معمولاً به منظور محدود کردن آزادی بیان، دسترسی به اطلاعات و حق تجمع به‌ویژه در دوران اعتراضات سیاسی، مانند آنچه در ایران دیده شده است، صورت می‌گیرد.

قطع اینترنت می‌تواند به صورت کامل باشند، که در آن دسترسی به تمامی بخش‌های شبکه‌ها قطع می‌شود، یا به صورت جزئی، که در آن بخشی شبکه یا خدمات خاصی مانند داده‌های تلفن همراه یا شبکه‌های اجتماعی هدف قرار می‌گیرند. روش‌هایی مانند کاهش عمدی پهنای باند، که در آن سرعت اینترنت به طور قابل توجهی کند می‌شود، نیز رایج است. قطع دسترسی به اینترنت ممکن است کل کشور یا مناطق خاصی را هدف قرار دهند و از چند ساعت تا چندین ماه به طول بینجامد.

اگرچه مقابله با قطع اینترنت دشوار است، اما راهکارهایی برای ارزیابی خطرات و کاهش تأثیرات آن وجود دارد. سازمان Access Now منابعی در این زمینه از طریق کمپین [KeepItOn#](#) ارائه می‌دهد.

برای افرادی که به دنبال منابعی برای آمادگی و مقابله با قطع اینترنت هستند، وبسایت «[ایران در خاموشی](#)» به عنوان یک مرکز منابع ارزشمند عمل می‌کند. این سایت آموزش‌های متنوعی در مورد ابزارهایی که در زمان قطعی یا اختلالات اینترنت می‌توانند مفید باشند، همراه با آموزش‌هایی برای آمادگی قبلی، ارائه می‌دهد. اطلاعات این سایت به زبان‌های مختلف از جمله فارسی، ترکی، عربی و بلوچی در دسترس است.

چکیده

این پژوهش به مقایسه چالش‌ها و نیازهای سه گروه کلیدی در ایران می‌پردازد: اقلیت‌های قومی (استان‌های بلوچستان، کردستان و استان‌های ترک‌نشین)، روزنامه‌نگاران تحقیقی و اقلیت‌های مذهبی (جامعه بهایی) در دوران قطع اینترنت. هر گروه با چالش‌های منحصربه‌فردی در ارتباط با دسترسی به ابزارهای ارتباطی امن، سطح آموزش در امنیت دیجیتال و خطرات خاصی که با آن مواجه هستند، روبرو می‌شوند. با این حال، شباهت‌هایی نیز بین این گروه‌ها وجود دارد، علاوه بر تفاوت‌های قابل توجه در سطح نیازها و خطرات.

مقایسه چالش‌ها

اقلیت‌های قومی: این گروه اجتماعی در دوران قطع اینترنت به شدت در انزوا قرار می‌گیرند، به‌ویژه بلوچ‌ها که در مقایسه با مناطق کردستان دسترسی کمتری به روش‌های جایگزین ارتباطی دارند. هر دو گروه به‌طور گسترده به VPN و تغییر سیم‌کارت برای دور زدن سانسور دولتی متکی هستند، اما در زمان قطع کامل اینترنت، گزینه‌های ارتباطی آن‌ها به شدت

محدود می‌شود. عدم آشنایی با ابزارهای امن یا سیستم‌های ماهواره‌ای (مانند توشه یا استارلینک) و شبکه‌های هم‌تا به هم‌تا (P2P) آسیب‌پذیری آن‌ها را تشدید می‌کند.

روزنامه‌نگاران تحقیقی: این گروه به دلیل اتکای زیاد به روش‌های ارتباطی ناامن، از جمله اسکایپ و سیم‌کارت‌های بین‌المللی، و همچنین عدم توجه به پروتکل‌های امنیت دیجیتال، به شدت آسیب‌پذیر هستند.

از سوی دیگر فعالیت‌های روزنامه‌نگاران در کشورهایی مانند ایران این گروه اجتماعی را در تقابل مستقیم با مقامات دولتی قرار می‌دهد؛ همین موضوع باعث ایجاد خطر فزاینده برای آن‌ها می‌شود. همچنین روزنامه‌نگاران به صورت پیوسته در معرض خطر بازداشت، احضار و توقیف وسائل الکترونیکی‌شان قرار دارند.

اقلیت‌های مذهبی: اقلیت‌های مذهبی به عنوان گروهی که غالباً توسط نهادهای امنیتی، قضایی و حتی دینی یا مذهبی مورد آزار و اذیت قرار می‌گیرد، با چالش‌های منحصربه‌فردی روبرو هستند. در حالی که برخی از آن‌ها با ابزارهایی مانند توشه آشنایی دارند، اتکای آن‌ها به تلفن‌های یک‌بار مصرف و VPN‌ها باعث می‌شود که در زمان قطع اینترنت آسیب‌پذیر باشند. این جامعه به صورت محدود به آموزش‌های سازمان‌دهی شده دسترسی دارد، اما این آموزش‌ها ناپیوسته بوده و عمق کافی برای محافظت کامل در برابر تهدیدات دیجیتال را ندارد.

ارزیابی تهدیدها و نیازسنجی

اولویت اول با ضرورت فوری: روزنامه‌نگاران تحقیقی بیشترین نیاز را به آموزش‌های پیشرفته امنیت دیجیتال و دسترسی به ابزارهای ارتباطی امن دارند. ماهیت کار آن‌ها باعث می‌شود که به طور خاص در معرض دید و آسیب‌پذیری نسبت به سرکوب حکومتی قرار بگیرند، و روش‌های کنونی آن‌ها حفاظت کافی در برابر خطراتی که با آن مواجه هستند را فراهم نمی‌کند. توسعه برنامه‌های آموزشی متناسب با نیازهای آن‌ها و معرفی ابزارهای امن‌تر برای این گروه حیاتی است.

اولویت دوم با ضرورت قابل توجه: اقلیت‌های قومی، به ویژه بلوچ‌ها، نیز با خطرات قابل توجهی مواجه هستند، به خصوص در دوران قطع کامل اینترنت. انزوای آن‌ها و عدم دسترسی به روش‌های جایگزین ارتباطی، آسیب‌پذیری‌شان را افزایش می‌دهد. اگرچه به اندازه روزنامه‌نگاران هدف مستقیم نیستند، اما آشنایی کم آن‌ها با ابزارهای امن در زمان افزایش نظارت دولتی، این گروه اجتماعی را در معرض خطر بالایی قرار می‌دهد.

اولویت سوم با ضرورت کمتر اما همچنان مهم: جامعه بهایی، اگرچه با خطرات فوری کمتری در مقایسه با دو گروه دیگر مواجه است، اما همچنان به آموزش‌های بهتر و منظم‌تری در زمینه امنیت دیجیتال نیاز دارد. روش‌های کنونی آن‌ها در مواقع افزایش آزار و اذیت، آن‌ها را آسیب‌پذیر می‌کند.

چالش‌های مشترک

آشنایی محدود با ابزارهای امن: در میان تمامی گروه‌ها، عدم آشنایی کافی با ابزارهای ارتباطی امن، از جمله سیستم‌های ماهواره‌ای (مانند استارلینک) و شبکه‌های «همتا به همتا»، به وضوح مشاهده می‌شود. این شکاف، توانایی آن‌ها برای حفظ ارتباطات در زمان قطع اینترنت را به‌طور جدی محدود می‌کند.

آموزش ناکافی: بیشتر شرکت‌کنندگان آموزش‌های کافی در زمینه امنیت دیجیتال دریافت نکرده‌اند. تقاضای زیادی برای آموزش جامع و مداوم، به‌ویژه در مورد استفاده از ابزارهای امن و کاهش خطراتی مانند فیشینگ و ضبط دستگاه‌های الکترونیکی توسط نهادهای امنیتی وجود دارد.

خطرات امنیتی: استفاده از روش‌های ارتباطی ناامن، مانند VPN‌های غیر امن نشده و اپلیکیشن‌های پیام‌رسان محبوب، خطرات قابل‌توجهی ایجاد می‌کند. از جمله احتمال دستیابی نهادهای امنیتی و قضایی به اطلاعات گروه‌های در معرض خطر، ضبط دستگاه‌های الکترونیکی فعالان که می‌تواند منجر به بازداشت و پیامدهای قانونی برای آن‌ها شود.

نیازهای منحصر به فرد

اقلیت‌های قومی: جوامع بلوچ و کرد معمولاً با چالش‌های مشابهی مانند وابستگی به VPN‌ها و تغییر سیم‌کارت برای دور زدن سانسور حکومتی مواجه هستند. با این حال، کردها از دسترسی نسبی به کانال‌های ارتباطی جایگزین از طریق اقلیم کردستان عراق برخوردارند، در حالی که بلوچستان در زمان قطع اینترنت با انزوای بیشتری مواجه است.

روزنامه‌نگاران تحقیقی: این گروه به ابزارهایی مانند اسکایپ و سیم‌کارت‌های بین‌المللی متکی هستند، اما به‌طور کلی به امنیت دیجیتال توجه کافی ندارند، که این امر آن‌ها را به‌شدت آسیب‌پذیر می‌کند. آن‌ها به آموزش‌های تخصصی برای بهبود رویه‌های امنیتی خود و دسترسی بهتر به ابزارهای ارتباطی امن نیاز دارند.

اقلیت‌های مذهبی: جامعه بهایی تا حدی با ابزارهای امن مانند توشه آشناست، اما به آموزش جامع و منظم دسترسی کافی ندارد. اتکای آن‌ها به تلفن‌های یک‌بار مصرف و VPN‌ها در زمان قطع اینترنت آن‌ها را به‌شدت آسیب‌پذیر می‌کند.

راهکارهای آتی

برای رفع این شکاف‌ها، توسعه نسخه دوم پروتکل قطع اینترنت باید بر موارد زیر متمرکز شود:

برنامه‌های آموزشی جامع: طراحی و اجرای برنامه‌های آموزشی متناسب با نیاز هر گروه برای افزایش شناخت و استفاده از ابزارهای ارتباطی امن. این برنامه‌ها باید شامل جلسات عملی در مورد استفاده از ارتباطات ماهواره‌ای، شبکه‌های هم‌تا به هم‌تا و پلتفرم‌های پیام‌رسان رمزگذاری شده باشد.

پروتکل‌های امنیتی: ایجاد دستورالعمل‌های روشن برای تأمین امنیت ارتباطات قبل، حین و پس از قطع اینترنت. این مورد نیز شامل گام‌های آماده‌سازی مانند آشنایی با ابزارها و شبکه‌های جایگزین و راه‌اندازی کانال‌های رمزگذاری شده، همچنین مستندسازی و استراتژی‌های بازیابی پس از قطع اینترنت می‌شود.

تأمین و توزیع ابزارهای جدید و پشتیبانی: اطمینان از دسترسی هر گروه به ابزارهای مناسب، مانند استارلینک و شبکه‌های مش (Mesh Networks)، و ارائه پشتیبانی مداوم برای کمک به آن‌ها در استفاده موثر از این ابزارها در شرایط خاص خود.

اعتمادسازی و پذیرش: توسعه ابتکارات جامعه محور برای ایجاد اعتماد به ابزارهای جدید و ترویج استفاده از آن‌ها؛ این هدف از طریق کارگاه‌های محلی، آموزش‌های هدایت‌شده توسط هم‌تایان و ایجاد شبکه‌های پشتیبانی محقق می‌شود. با پرداختن به این مسائل، نسخه به‌روزشده پروتکل بهتر می‌تواند این گروه‌ها را برای مقابله با چالش‌های ناشی از قطع اینترنت آماده کند و اطمینان حاصل شود که ارتباطات آن‌ها امن و مقاوم باقی می‌ماند.

مدل‌سازی تهدیدها: راهکارهای پیشگیرانه و مقابله‌ای

در بستر قطع اینترنت در ایران، گروه‌های اجتماعی مختلفی از جمله اقلیت‌های قومی، روزنامه‌نگاران تحقیقی و اقلیت‌های مذهبی با چالش‌های قابل توجهی برای حفظ ارتباطات امن مواجه هستند. «مدل‌سازی تهدیدات» به معنای شناسایی و درک خطرات خاص برای هر یک از این گروه‌ها و تهیه راهبردهایی برای کاهش مؤثر این تهدیدها است.

شناسایی تهدیدها

تهدیدات اصلی که این گروه‌ها در زمان قطع اینترنت با آن مواجه هستند، عبارتند از:

نظارت: حکومت ایران به‌طور فعال ارتباطات را به‌ویژه در زمان‌های ناآرامی‌های مدنی یا اعتراضات رصد می‌کند. این موضوع خطر بزرگی برای تمامی گروه‌ها، به‌ویژه روزنامه‌نگاران تحقیقی و اقلیت‌های قومی، که اغلب در فعالیت‌هایی دخیل هستند که موجب جلب توجه حکومت یا نهادهای امنیتی می‌شود، ایجاد می‌کند.

ضبط و مصادره دستگاه‌های الکترونیکی: ضبط فیزیکی دستگاه‌های الکترونیکی توسط مقامات یک امر رایج است، به‌ویژه برای روزنامه‌نگاران و فعالان در جوامع بلوچ و کرد. دستگاه‌های ضبط شده می‌توانند منجر به افشای اطلاعات حساس، تماس‌ها و ارتباطاتی باشند که ممکن است به بازداشت، محکومیت یا آزار بیشتر منتهی می‌شوند.

روش‌های ارتباطی ناامن: اتکای گروه‌های در معرض خطر به VPN‌های تایید نشده، اپلیکیشن‌های پیام‌رسان محبوبی مانند واتساپ و سیم‌کارت‌های بین‌المللی ناامن آن‌ها را در معرض نظارت، رهگیری ارتباطات و افشای اطلاعات قرار می‌دهد.

عدم دسترسی به ابزارهای امن: دسترسی محدود به ابزارهای ارتباطی امن، مانند سیستم‌های مخابراتی (مثل استارلینک) و شبکه‌های هم‌تا به هم‌تا، آسیب‌پذیری این گروه‌ها را افزایش می‌دهد. جامعه بهایی، اگرچه کمتر هدف مستقیم قرار می‌گیرد، همچنان به دلیل آموزش ناکافی و دسترسی نامنظم به روش‌های ارتباطی امن با مشکلاتی مواجه است.

تجزیه و تحلیل نقاط آسیب‌پذیر

هر گروه دارای آسیب‌پذیری‌های خاصی بر اساس دسترسی به منابع، سطح آموزش و نوع تهدیداتی که با آن مواجه هستند:

اقلیت‌های قومی: این گروه از شهروندان به دلیل انزوا و نداشتن دسترسی به روش‌های جایگزین ارتباطی در زمان قطع اینترنت، به‌شدت آسیب‌پذیر هستند. اتکای شدید به VPN‌ها و تغییر سیم‌کارت، آن‌ها را در معرض نظارت حکومتی قرار داده و آشنایی محدود با ابزارهای امن، خطر را برایشان بیشتر می‌کند.

روزنامه‌نگاران تحقیقی: این گروه به دلیل جلب توجه بالا و فعالیت آشکار و ماهیت حساس کار خود به‌شدت آسیب‌پذیر هستند. استفاده از روش‌های ارتباطی ناامن و عدم توجه کافی به رویه‌های امنیت دیجیتال آن‌ها را به هدف اصلی سرکوب دولتی، نظارت و ضبط دستگاه‌ها تبدیل کرده است.

اقلیت‌های مذهبی: جامعه بهایی، اگرچه کمتر به‌طور مستقیم هدف قرار می‌گیرد، همچنان به دلیل آموزش‌های ناپیوسته و اتکای آن‌ها به ابزارهای ارتباطی ناامن در معرض خطر است. راهکارهای اعضای این جامعه در زمان‌های بحرانی، به‌ویژه در دوران قطع اینترنت، محدود و مخاطره‌آمیز می‌شود.

آمادگی برای تهدیدات

برای کاهش تهدیدات، هر گروه باید گام‌های خاصی را برای بهبود امنیت و مقاومت خود در زمان قطع اینترنت بردارد:

آموزش جامع: اجرای برنامه‌های آموزشی متناسب با نیازهای هر گروه تمرکز بر رویه‌های امنیت دیجیتال، روش‌های ارتباطی امن و آگاهی از تهدیدات.

برای استفاده از ابزارهای جایگزین ارتباطی مانند شبکه‌های مش و سیستم‌های مخابراتی باشد. روزنامه‌نگاران، اما بیشتر نیاز به اطلاعات در رابطه با پیام‌رسانی امن، رمزگذاری و حفاظت از داده‌ها دارند. جامعه بهایی نیز از آموزش‌های منظم و سازماندهی‌شده در مورد استفاده ایمن از ابزارهای ارتباطی و رویه‌های امنیت دیجیتال بهره‌مند خواهد شد.

دسترسى به ابزارهاى امن: اطمینان از دسترسى همه گروه‌ها به ابزارهاى ارتباطى امن مانند استارلینک، پلتفرم‌هاى پیام‌رسانى رمزگذاری شده و شبکه‌هاى هم‌تا به هم‌تا. ارائه این ابزارها همراه با پشتیبانى مداوم برای اطمینان از استفاده صحیح از آن‌ها به کاهش خطرات نظارت حکومتى و قطع ارتباطات کمک مى‌کند.

ایجاد اعتماد و پذیرش: ایجاد اعتماد در میان این جوامع برای پذیرش ابزارها و رویه‌هاى امنیتی جدید ضرورى است. این امر از طریق ابتکارات جامعه‌محور، آموزش‌هاى هدایت‌شده توسط هم‌ترازان و ایجاد شبکه‌هاى پشتیبانى که راهنمائی و پشتیبانى مداوم ارائه مى‌دهند، قابل دستیابی است.

ایجاد پروتکل‌هاى امنیتی: باید پروتکل‌هاى امنیتی روشن برای ارتباطات قبل، حین و بعد از قطع اینترنت تدوین شود. این پروتکل‌ها شامل گام‌هاىی برای تأمین امنیت دستگاه‌ها، حفاظت از داده‌ها و اطمینان از ارتباطات امن است. به‌روزرسانى‌ها و یادآورى‌هاى منظم درباره این پروتکل‌ها مى‌تواند اهمیت و اثربخشى آن‌ها را تقویت کند.

استفاده از منابع خارجى: پلتفرم‌هاىی مانند [ایران در خاموشی](http://irandarkhamooshi.net) منابع ارزشمندی برای آمادگی و مدیریت قطع اینترنت ارائه مى‌دهند. این منابع که به زبان‌هاى مختلف در دسترس هستند، آموزش‌هاىی در مورد ابزارهاى مفید و راهبردهاىی برای کاهش تأثیرات قطع اینترنت ارائه مى‌کنند.

پایش و هماهنگى مداوم

مدل‌سازى تهدیدات یک فرآیند مداوم است که نیاز به نظارت مستمر بر وضعیت تهدیدات و انطباق راهبردها با ظهور خطرات جدید دارد. هر گروه اجتماعى باید به‌طور منظم آسیب‌پذیری‌هاى خود و اثربخشى استراتژی‌هاى کاهش تهدیدات را ارزیابی کند و در صورت لزوم تغییراتی اعمال کند تا همیشه یک قدم جلوتر از تهدیدات احتمالى باشد.

با در نظر گرفتن تمامی این موارد این جوامع آسیب‌پذیر مى‌توانند برای مقابله با چالش‌هاى ناشی از قطع اینترنت بهتر آماده شوند و ارتباطات خود را تا حد ممکن امن و مقاوم نگه دارند.

برنامه‌ریزی

برنامه‌ریزی برای اقدامات قبل از قطع اینترنت، در طول دوره قطع و پس از آن، برای تضمین تاب‌آورى و تداوم فعالیت‌ها در این دوره بسیار حیاتی است.

آمادگی پیش از قطع اینترنت شامل راه‌اندازى ابزارها، برقرارى ارتباطات امن و سیستم‌هاى پشتیبان‌گیری از داده‌ها برای کاهش تأثیر احتمالى قطع اینترنت است. اقدامات در طول دوره قطع اینترنت بر حفظ دسترسى به اطلاعات حیاتی، مستندسازی وقایع و یافتن کانال‌هاى ارتباطى جایگزین تمرکز دارد. اقدامات پس از قطع اینترنت برای بازیابی داده‌ها، تحلیل تأثیرات قطع اینترنت و تلاش برای بازگرداندن خدمات ضرورى است.

این گام‌ها به محافظت از داده‌ها، اطمینان از ارتباطات و واکنش مؤثر به اختلالات کمک مى‌کنند.

آمادگی پیش از قطع اینترنت

برای آماده‌سازی مؤثر در برابر قطع اینترنت، ضروری است که اقدامات پیشگیرانه‌ای برای تقویت امنیت، اطمینان از تداوم ارتباطات و کاهش تأثیرات اختلالات صورت بگیرد. اقدامات زیر باید انجام شود:

برنامه‌های آموزشی جامع

- **آموزش امنیت دیجیتال:** آموزش به گروه‌های مدنظر در زمینه اصول و تکنیک‌های پیشرفته امنیت دیجیتال، از جمله روش‌های ارتباطی امن، رمزگذاری و چگونگی شناسایی حملات فیشینگ.
- **آشنایی با ابزارها:** ارائه آموزش عملی برای استفاده از ابزارهای ارتباطی امن همچون سیستم‌های ماهواره‌ای (مانند استارلینک)، شبکه‌های مش و پلتفرم‌های پیام‌رسان رمزگذاری شده. حصول اطمینان از اینکه شرکت‌کنندگان قبل از قطع اینترنت، نحوه راه‌اندازی و استفاده مؤثر از این ابزارها را می‌دانند.

دسترسی به ابزارهای امن و توزیع آن‌ها

- **توزیع ابزارهای امن:** اطمینان حاصل کنید که افراد و سازمان‌ها به ابزارهای لازم، مانند دستگاه‌های استارلینک، تنظیمات شبکه مش و اپلیکیشن‌های پیام‌رسان امن دسترسی دارند. این ابزارها را به‌طور گسترده در جوامع در معرض خطر توزیع کنید.
- **منابع آفلاین:** دسترسی به منابعی که می‌توانند به‌صورت آفلاین استفاده شوند را فراهم کنید، مانند راهنماهای PDF در زمینه امنیت دیجیتال، دستگاه‌های ذخیره‌سازی رمزگذاری‌شده برای اطلاعات حساس و نسخه‌های فیزیکی از اطلاعات مهم.

ایجاد پروتکل‌های ارتباطی

- **پروتکل‌های قبل از قطع اینترنت:** پروتکل‌های ارتباطی روشن و قابل فهمی را توسعه دهید که مراحل لازم قبل، حین و بعد از قطع اینترنت را شرح می‌دهد. این پروتکل‌ها باید شامل راه‌های جایگزین برای ارتباطات، مانند استفاده از رادیو، پیامک یا شبکه‌های محلی باشد.
- **طرح‌های ارتباطی پشتیبان:** روش‌های ارتباطی پشتیبانی که به اینترنت متکی نیستند، مانند اپلیکیشن‌های پیام‌رسان هم‌تا به هم‌تا، ایجاد کنید. اطمینان حاصل کنید که این روش‌ها تست شده و توسط تمام کاربران درک شده‌اند.

ایجاد شبکه‌های اجتماعی محلی

- **شبکه‌های جامعه محور:** آن دسته از شبکه‌های محلی را تقویت کنید که می‌توانند به‌طور مستقل از اینترنت عمل کنند. تشکیل گروه‌های محلی برای اشتراک‌گذاری اطلاعات و منابع در زمان قطع اینترنت را تشویق کنید.
- **ایجاد اعتماد:** اعتماد به استفاده از ابزارها و روش‌های جدید در جامعه را تقویت کنید. جلسات آموزشی هدایت‌شده توسط گروه‌های مرتبط و کارگاه‌های محلی می‌توانند به افزایش اعتماد و پذیرش گسترده شیوه‌های امن کمک کنند.

پیش‌بینی و آماده‌سازی اطلاعات

- **توزیع اطلاعات:** اطلاعات ضروری را درباره آنچه باید در صورت قطع اینترنت انجام شود قبل از وقوع آن توزیع کنید. این اطلاعات شامل دستورالعمل‌هایی برای استفاده از ابزارهای آفلاین، راه‌اندازی شبکه‌های جایگزین و تأمین امنیت دستگاه‌ها باشد.
- **محتوای بومی‌سازی‌شده:** اطمینان حاصل کنید که تمام مواد به زبان‌های محلی و متناسب با فرهنگ منطقه در دسترس است. وبسایت‌هایی مانند [ایران در خاموشی](#) منابعی را به زبان‌های فارسی، ترکی، عربی و بلوچی برای آموزش و آماده‌سازی جوامع متنوع فراهم می‌کنند.

تمرین‌ها و شبیه‌سازی‌های منظم

- **شبیه‌سازی سناریوهای قطع اینترنت:** تمرین‌های منظم برای شبیه‌سازی قطع اینترنت انجام دهید تا جوامع بتوانند استفاده از روش‌ها و ابزارهای ارتباطی امن خود را در محیطی کنترل‌شده تمرین کنند.
 - **ارزیابی و هماهنگی:** پس از هر تمرین، اثربخشی ابزارها و پروتکل‌ها را ارزیابی کرده، بازخوردها را جمع‌آوری کنید و اصلاحات لازم را برای بهبود آمادگی انجام دهید.
- با اجرای این مراحل آماده‌سازی پیش از قطع اینترنت، گروه‌های یادشده به شکل بهتری قادر خواهند بود تا ارتباطات خود را حفظ کنند، از امنیت دیجیتال خود محافظت کرده و حتی در مواجهه با قطع اینترنت به فعالیت‌های خود ادامه دهند.

در دوره قطعی اینترنت

هنگام وقوع قطع اینترنت، ضروری است که راهکارهایی اتخاذ شود شوند تا ارتباطات ادامه یابند، امنیت حفظ شود و اختلال در فعالیت‌های حیاتی به کمترین میزان ممکن برسد. در اینجا اقداماتی که در طول قطع اینترنت باید انجام شوند، آورده شده است:

فعال‌سازی روش‌های ارتباطی پشتیبان

- **استفاده از شبکه‌های جایگزین:** روش‌های ارتباطی جایگزینی که از پیش آماده شده‌اند، مانند شبکه‌های مش، تلفن‌های ماهواره‌ای، رادیوهای دستی یا اپلیکیشن‌های پیام‌رسان هم‌تا به هم‌تا (مانند Briar یا Bridgefy) را به کار بگیرید. این ابزارها بدون تکیه بر زیرساخت‌های سنتی اینترنت کار می‌کنند.
- **ارتباط از طریق پیامک و تماس صوتی:** اگر شبکه‌های تلفن همراه همچنان فعال هستند، از پیامک و تماس‌های صوتی برای ارتباطات ضروری استفاده کنید. این روش‌ها در قطع‌های جزئی اینترنت از خدمات پیام‌رسانی مبتنی بر اینترنت قابل اعتمادتر هستند.

حفظ پروتکل‌های امنیتی

- **رمزگذاری ارتباطات:** اطمینان حاصل کنید که تمام ارتباطات، چه از طریق شبکه‌های جایگزین و چه از طریق پیامک، رمزگذاری شده باشند. از اپلیکیشن‌ها و ابزارهایی که از رمزگذاری سرتاسری پشتیبانی می‌کنند برای محافظت از اطلاعات حساس استفاده کنید.
- **امنیت دستگاه‌های الکترونیکی:** از تأمین امنیت دستگاه‌های الکترونیکی غافل نشوید. سرویس‌های غیرضروری (مانند GPS یا بلوتوث) را در صورت عدم نیاز غیرفعال کنید، از رمزهای عبور قوی استفاده کنید و در مورد امنیت فیزیکی دستگاه‌ها احتیاط کنید (برای مثال، دستگاه‌ها را در مکان‌های امن نگهداری کنید).
- **اجتناب از ابزارهای ناامن:** از استفاده از اپلیکیشن‌ها و خدمات ناامن یا تحت نظارت خودداری کنید، زیرا ممکن است توسط نهادهای امنیتی یا حکومتی رصد شوند.

ایجاد و استفاده از محل‌های ملاقات امن

- **مکان‌های ملاقات حضوری:** اگر ابزارهای ارتباطی به شدت محدود شده‌اند، مکان‌های ملاقات حضوری را از پیش تعیین کنید که افراد بتوانند در محل‌ها به‌طور امن برای تبادل اطلاعات و هماهنگی فعالیت‌ها ملاقات کنند. اطمینان حاصل کنید که این مکان‌ها از شاخص‌های لازم برای «امن» تلقی شدن برخوردار باشند.
- **اشتراک‌گذاری اطلاعات آفلاین:** از روش‌های فیزیکی برای به اشتراک گذاشتن اطلاعات مهم استفاده کنید، مانند موارد چاپ شده، یادداشت‌های دستی یا حافظه‌های موسوم به فلش مموری. اطمینان حاصل کنید که این اطلاعات به‌طور ایمن و محرمانه به اشتراک گذاشته می‌شوند.

پایش وضعیت و هماهنگی

- **پایش لحظه‌ای:** به‌طور مستمر وضعیت قطع اینترنت را بررسی کنید، از جمله شبکه‌ها یا خدماتی که تحت تأثیر قرار گرفته‌اند. این کار را از طریق گزارش‌های محلی، شنیده‌ها یا استفاده از ابزارهایی مانند Ceno یا Lantern که ممکن است همچنان با ظرفیت محدود کار کنند، انجام دهید.
- **تطبیق روش‌های ارتباطی:** انعطاف‌پذیر باشید و روش‌های ارتباطی خود را براساس وضعیت موجود تطبیق دهید. به عنوان مثال، اگر یک شبکه جایگزین خاص تحت نظارت یا غیرقابل اعتماد شد، به روش دیگری تغییر دهید.

مستندسازی و گزارش‌دهی

- **جمع‌آوری شواهد:** تأثیرات قطع اینترنت را به‌طور ایمن مستندسازی کنید، از جمله اختلال در ارتباطات، نقض حقوق و هرگونه وقوع سرکوب یا خشونت. از روش‌های امن برای ذخیره‌سازی و به اشتراک‌گذاری این اطلاعات استفاده کنید.
- **گزارش مشکلات:** در صورت امکان، تأثیرات قطع اینترنت را به سازمان‌هایی که قطع‌ها را پایش و برای جلوگیری از آن‌ها تلاش می‌کنند، مانند Access Now، گزارش دهید. از کانال‌های امن برای ارسال گزارش‌ها و به‌روزرسانی‌ها استفاده کنید تا از شناسایی شدن جلوگیری شود.

حمایت از شبکه‌های محلی

- **تقویت پشتیبانی محلی:** در طول قطع اینترنت، به شبکه‌های اجتماعی محلی برای پشتیبانی تکیه کنید. منابع، اطلاعات و کمک‌های خود را با افرادی که ممکن است آسیب‌پذیرتر یا منزوی‌تر باشند، به اشتراک بگذارید.
- **هماهنگی محلی:** با اعضای کلیدی و فعال جامعه همکاری کنید تا تلاش‌های گروهی را سازمان‌دهی کرده و مطمئن شوید که همه افراد به ابزارها و اطلاعات ضروری دسترسی دارند.

آگاه ماندن

- **استفاده از منابع مطمئن:** به منابع اطلاعاتی معتبر تکیه کنید، هم در سطح محلی و هم از طریق هر کانال بین‌المللی موجود. مراقب شایعات یا اطلاعات نادرستی باشید که ممکن است در زمان قطع اینترنت منتشر شوند.
 - **به‌روزرسانی منظم:** پس از بازگشت ارتباطات، جامعه و شبکه‌های خود را از وضعیت به‌روز و تغییرات مربوط به قطع اینترنت یا تحولات جدید مطلع کنید.
- با دنبال کردن این مراحل در طول قطع اینترنت، گروه‌های اجتماعی می‌توانند سطحی از ارتباطات را حفظ کنند، امنیت دیجیتال و فیزیکی خود را محافظت کرده و فعالیت‌های حیاتی خود را علی‌رغم اختلالات ادامه دهند.

اقدامات پس از قطع اینترنت

پس از پایان قطع اینترنت، بسیار مهم است که اقداماتی برای بازیابی، ارزیابی تأثیرات و آمادگی برای اختلالات احتمالی در آینده انجام شود. در اینجا اقداماتی که باید پس از یک قطع اینترنت انجام شود، آمده است:

مستندسازی تأثیرات

- **جمع‌آوری و نگهداری شواهد:** تمام مستندات از جمله گزارش‌ها، اسکرین‌شات‌ها، ویدیوها و شهادت‌های مربوط به دوران قطع اینترنت را جمع‌آوری و به صورت امن نگهداری کنید تا از آن‌ها برای اقدامات آتی حقوقی یا مدنی استفاده شود.
- **ارزیابی تأثیرات:** تأثیرات قطع اینترنت بر جامعه یا سازمان خود را ارزیابی کنید. این امر شامل بررسی اختلال در ارتباطات، دسترسی به خدمات ضروری، تأثیرات اقتصادی و هرگونه نقض حقوق بشر است.

گزارش‌دهی و اشتراک اطلاعات

- **ارسال گزارش‌ها:** گزارش‌های دقیق درباره تأثیرات قطع اینترنت را با سازمان‌های حقوق بشر محلی و بین‌المللی مانند Access Now، عفو بین‌الملل یا سازمان ملل متحد به اشتراک بگذارید. از کانال‌های امن برای ارسال این گزارش‌ها استفاده کنید تا هویت افراد درگیر، محافظت شود.
- **آگاهی‌رسانی عمومی:** با به اشتراک‌گذاری یافته‌های خود با جامعه در سطحی گسترده‌تر، چه به صورت محلی و چه بین‌المللی، درباره قطع اینترنت آگاهی‌رسانی کنید. این اقدام می‌تواند حمایت و فشار برای جلوگیری از قطع‌های آینده را افزایش دهد.

بازبینی و به‌روزرسانی پروتکل‌های امنیتی

- ارزیابی اثربخشی پروتکل‌ها: نحوه عملکرد پروتکل‌های قبل و در طول قطع اینترنت را تحلیل کنید. هرگونه نقص یا ضعف در واکنش‌های خود را شناسایی کرده و برای بهبود آمادگی‌های آینده اصلاحات لازم را انجام دهید.
- به‌روزرسانی ابزارها و روش‌ها: بر اساس ارزیابی خود، ابزارها، روش‌ها و پروتکل‌ها را برای رفع آسیب‌پذیری‌های شناسایی شده به‌روزرسانی کنید. این ممکن است شامل دریافت فناوری‌های جدید، بهبود روش‌های ارتباطی یا ارائه آموزش‌های بیشتر باشد.

حمایت و جلسات بازنگری

- جلسات بازنگری جامعه: جلسات بازنگری با جامعه ارتباطی یا تیم خود برگزار کنید تا تجربیات قطع اینترنت را مورد بحث قرار دهید. این کار می‌تواند به افراد کمک کند تا تجربه خود را پردازش کرده، تجربیاتشان را به اشتراک بگذارند و ایده‌هایی برای بهبود آینده ارائه دهند.
- ارائه حمایت روانی: برای افرادی که به‌طور خاص تحت تأثیر قطع اینترنت قرار گرفته‌اند، مانند افرادی که با تهدید، بازداشت یا اشکال دیگر سرکوب مواجه شده‌اند، دسترسی به حمایت روانی فراهم کنید.

تقویت شبکه‌های اجتماعی محلی

- تقویت شبکه‌های محلی: از دوره پس از قطع اینترنت برای تقویت شبکه‌های پشتیبانی محلی که در طول قطع فعال شده بودند، استفاده کنید. اعتماد و همکاری درون جامعه را از طریق حل مشکلاتی که در طول قطع اینترنت به وجود آمدند، تقویت کنید.
- گسترش شبکه‌ها: تلاش کنید تا شبکه خود را گسترش دهید تا افراد و سازمان‌های بیشتری را که ممکن است در قطع‌های آینده تحت تأثیر قرار بگیرند، دربرگیرد. ایجاد شبکه‌ای بزرگتر و مقاوم‌تر می‌تواند آمادگی و توانایی‌های پاسخگویی را بهبود بخشد.

تلاش برای اصلاح سیاست‌ها

- مشارکت در فعالیت‌های حقوقی: از مستندات و گزارش‌های جمع‌آوری شده در طول قطع اینترنت در مسیر تلاش برای اصلاح سیاست‌ها در سطوح ملی و بین‌المللی استفاده کنید. برای تقویت حفاظت در برابر قطع اینترنت و به رسمیت شناختن دسترسی به اینترنت به عنوان یک حق انسانی اساسی تلاش کنید.
- همکاری با افراد و سازمان‌های هم‌سو: با سایر سازمان‌ها، چه به‌صورت محلی و چه جهانی، همکاری کنید تا تلاش‌های حقوقی خود را تقویت کنید. اقدام جمعی می‌تواند فشار بیشتری بر دولت‌ها وارد کند تا از قطع‌های آینده اجتناب کرده و حقوق دیجیتال را رعایت کنند.

آمادگی برای قطع‌های آینده

- بازبینی و تقویت برنامه‌های آمادگی: بر اساس تجربیات قطع اخیر، برنامه‌های آمادگی خود را بازبینی و تقویت کنید. اطمینان حاصل کنید که جامعه یا سازمان شما بهتر برای مقابله با اختلالات آینده مجهز شده است.

- **برگزاری آموزش و تمرین‌ها:** آموزش‌های بیشتری ارائه دهید تا همه با پروتکل‌ها و ابزارهای به‌روزشده آشنا شوند. تمرین‌های منظم برای شبیه‌سازی سناریوهای قطع اینترنت و تمرین پاسخ‌ها برگزار کنید.
- با انجام این اقدامات پس از قطع اینترنت، می‌توانید به جامعه یا سازمان خود کمک کنید تا از اختلالات بازیابی شود، تاب‌آوری خود را تقویت کند و برای هرگونه قطع اینترنت احتمالی در آینده بهتر آماده شود.

اولویت بندی آموزش

اولویت‌بندی آموزش برای آمادگی و واکنش به قطع اینترنت شامل تمرکز بر مهارت‌ها و دانش‌های حیاتی است که بیشترین تاثیر را بر تاب‌آوری و امنیت جامعه خواهند داشت. در ادامه، یک رویکرد پیشنهادی برای اولویت‌بندی آموزش ارائه شده است:

بررسی ضعف‌های کلیدی

- **ارزیابی دانش فعلی:** ابتدا سطح فعلی آگاهی از امنیت دیجیتال و مهارت‌های فنی در جامعه یا سازمان را ارزیابی کنید. کمبودهای مهارتی را که ممکن است منجر به آسیب‌پذیری در زمان قطع اینترنت شود، شناسایی کنید.
- **درک تهدیدات خاص:** آموزش را بر اساس تهدیدات خاص هر گروه مانند نظارت دولتی، ضبط دستگاه‌ها یا ناتوانی در برقراری ارتباط امن در زمان قطع اینترنت تنظیم کنید.

تمرکز بر مهارت‌های ضروری

- **امنیت دیجیتال پایه:** اولویت آموزش باید بر روی اصول امنیت دیجیتال باشد، مانند تنظیم رمزهای عبور قوی، استفاده از احراز هویت دو مرحله‌ای و شناسایی حملات فیشینگ. این مهارت‌های پایه برای همه کاربران ضروری است.
- **ابزارهای ارتباطی امن:** آموزش فوری درباره استفاده از ابزارهای ارتباطی امن که در زمان قطع اینترنت کار می‌کنند ارائه دهید، مانند اپلیکیشن‌های پیام‌رسان رمزگذاری‌شده، شبکه‌های مش و سیستم‌های ارتباطی ماهواره‌ای.

آموزش متناسب با نیازهای خاص

- **اقلیت‌های قومی:** آموزش‌هایی ارائه دهید که توانایی این گروه اجتماعی در برقراری ارتباط امن در زمان قطع کامل یا جزئی اینترنت را بهبود بخشد. این شامل استفاده از روش‌های جایگزین مانند تلفن‌های ماهواره‌ای یا شبکه‌های مش و درک چگونگی اجتناب از نظارت است.
- **روزنامه‌نگاران تحقیقی:** آموزش‌های پیشرفته امنیت دیجیتال مانند رمزگذاری، ذخیره‌سازی امن داده‌ها و شیوه‌های گزارش‌دهی امن را در اولویت قرار دهید. روزنامه‌نگاران به دلیل ریسک بالای شغلی خود به مهارت‌های پیشرفته‌تری برای محافظت از کار و منابع خود نیاز دارند.
- **اقلیت‌های مذهبی:** آموزش‌ها را بر روی شیوه‌های ارتباط امن متمرکز کنید تا از جامعه آن‌ها در دوران افزایش آزار و اذیت محافظت شود. اطمینان حاصل کنید که آن‌ها با ابزارهایی آشنا هستند که بتوانند در زمان هدف قرار گرفتن، ارتباطات داخلی را حفظ کنند.

اجرای جلسات عملی آموزشی

- **کارگاه‌های عملی:** کارگاه‌های عملی برگزار کنید تا شرکت‌کنندگان بتوانند ابزارها و روش‌هایی را که یاد گرفته‌اند، تمرین کنند. این کار اطمینان می‌دهد که آن‌ها نه تنها از نظر تئوریک آماده هستند، بلکه از نظر عملی نیز توانایی لازم را دارند.
- **تمرین‌های مبتنی بر سناریو:** تمرین‌هایی که سناریوی قطع اینترنت را شبیه‌سازی می‌کنند اجرا کنید. این کار به شرکت‌کنندگان کمک می‌کند تا در زمان واقعی واکنش نشان دهند و هرگونه نیاز به آموزش بیشتر را مشخص کنند.

گسترش منابع آموزشی مستمر

- **دسترسی به پشتیبانی مستمر:** منابع آموزشی مداوم مانند آموزش‌های آنلاین، راهنماها و انجمن‌هایی که افراد می‌توانند سؤالات خود را مطرح کرده و تجربیات خود را به اشتراک بگذارند، ارائه دهید.
- **مواد آموزشی بومی‌سازی شده:** اطمینان حاصل کنید که مواد آموزشی به زبان‌های محلی در دسترس هستند و برای همه اعضای جامعه قابل فهم باشند. از منابعی مانند [ایران در خاموشی](http://irandarkhamooshi.net) برای ارائه اطلاعات خاص منطقه استفاده کنید.

ارزیابی و انطباق برنامه‌های آموزشی

- **بازخورد مستمر:** به‌طور منظم از شرکت‌کنندگان بازخورد جمع‌آوری کنید تا اثربخشی آموزش را ارزیابی کنید. از این بازخورد برای انجام تنظیمات لازم در محتوای آموزشی یا روش‌های ارائه استفاده کنید.
- **به‌روزرسانی منظم آموزش‌ها:** با ظهور تهدیدات جدید یا در دسترس قرار گرفتن ابزارهای جدید، برنامه‌های آموزشی را به‌روزرسانی کنید تا همیشه مرتبط و مؤثر باقی بمانند.

ایجاد اعتماد و تعامل

- **ابتکارات مبتنی بر جامعه:** جلسات آموزشی هدایت‌شده توسط هم‌تایان و یادگیری مبتنی بر جامعه را ترویج دهید. زمانی که آموزش توسط اعضای معتمد جامعه ارائه شود، پذیرش و به‌کارگیری آن افزایش می‌یابد.

- **فعالیت‌های مشارکتی:** از رویدادهای اجتماعی، بحث‌ها و کارگاه‌ها برای حفظ تعامل و علاقه جامعه به یادگیری مداوم و آماده‌سازی استفاده کنید.

با دنبال کردن این مراحل، می‌توانید اطمینان حاصل کنید که آموزش به‌طور مؤثری اولویت‌بندی شده و بر نیازهای حیاتی تمرکز دارد. این کار به ایجاد پایه‌ای قوی از دانش و مهارت‌ها کمک می‌کند که باعث می‌شود جامعه یا سازمان در طول و پس از قطع اینترنت مقاوم‌تر باشد.

ابزارهای ارتباط امن و همتا به همتا (P2P)

در زمینه ارتباطات امن و ابزارهای همتا به همتا (P2P)، نکته کلیدی این است که از ابزارهایی استفاده شود که قابل اعتماد، کاربرپسند و در برابر نظارت و رهگیری ایمن باشند. در اینجا برخی از پیشنهادها ارائه شده است:

اپلیکیشن‌های پیام‌رسان امن

این اپلیکیشن‌ها رمزگذاری سرتاسری ارائه می‌دهند و برای محافظت از ارتباطات حتی در محیط‌های پرخطر طراحی شده‌اند:

- **سیگنال:** یکی از امن‌ترین اپلیکیشن‌های پیام‌رسان موجود است که برای ارتباطات متنی، صوتی و ویدیویی رمزگذاری سرتاسری ارائه می‌دهد. این اپلیکیشن منبع‌باز است و در جامعه امنیتی به‌شدت مورد اعتماد است و استفاده از آن آسان است.
- **واتس‌آپ:** با وجود این که رمزگذاری سرتاسری ارائه می‌دهد و به‌طور گسترده استفاده می‌شود، به دلیل مالکیت آن توسط متا (Meta)، نگرانی‌هایی در مورد حریم خصوصی وجود دارد. با این حال، برای ارتباطات روزمره و در بسیاری از مناطق گزینه‌ای محبوب و نسبتاً امن است.
- **تلگرام:** ارتباطات رمزگذاری شده ارائه می‌دهد، اما تنها در حالت «چت محرمانه» (Secret Chat) این رمزگذاری فعال است. این اپلیکیشن به‌طور گسترده در مناطقی با سانسور اینترنت استفاده می‌شود، اگرچه رمزگذاری آن نسبت به سیگنال ضعیف‌تر است.

ابزارهای ارتباط همتا به همتا (P2P)

ابزارهای P2P در زمان قطع اینترنت اهمیت ویژه‌ای دارند، زیرا بدون نیاز به سرورهای مرکزی کار می‌کنند و در برابر کنترل‌های دولتی مقاوم‌تر هستند:

- **Briar:** یک اپلیکیشن پیام‌رسان P2P بسیار امن است که از طریق بلوتوث، وای‌فای یا اینترنت کار می‌کند. این اپلیکیشن برای فعالان و روزنامه‌نگاران طراحی شده و حتی زمانی که اینترنت قطع است با شبکه‌های محلی کار می‌کند.
- **Bridgefy:** این اپلیکیشن به کاربران اجازه می‌دهد از طریق بلوتوث ارتباط برقرار کنند و یک شبکه مش ایجاد کنند که دستگاه‌ها را مستقیماً به هم متصل می‌کند. این ابزار در شرایطی که اینترنت در دسترس نیست اما کاربران در نزدیکی هم قرار دارند، مفید است.

- **Delta Chat** : این ابزار تلفیقی از قابلیت‌های ایمیل سنتی و پیام‌رسانی فوری است و به عنوان یک ابزار ارتباط امن در زمان قطع اینترنت بسیار مفید است.

سرویس‌های ایمیل امن

برای ارتباطات ایمیلی امن، به ویژه هنگام ارسال اسناد حساس:

- **ProtonMail** : این سرویس ایمیل مبتنی بر سوئیس رمزگذاری سرتاسری و حفاظت‌های قوی حریم خصوصی ارائه می‌دهد و گزینه‌ای مناسب برای ارسال اطلاعات حساس به صورت امن است.
- **Tutanota** : یک سرویس ایمیل امن دیگر که رمزگذاری سرتاسری ارائه می‌دهد، کاربرپسند است و ویژگی‌هایی مانند تقویم‌های رمزگذاری‌شده نیز ارائه می‌دهد.

شبکه‌های مش

شبکه‌های مش شبکه‌های غیرمتمرکزی هستند که حتی در زمان قطع اینترنت امکان ارتباطات را حفظ می‌کنند:

- **goTenna Mesh** : دستگاه‌های goTenna Mesh یک شبکه ارتباطی خصوصی و خارج از شبکه اینترنت با استفاده از امواج رادیویی برد بلند ایجاد می‌کنند. این دستگاه‌ها در مناطق بدون پوشش شبکه یا در زمان قطع اینترنت بسیار کارآمد هستند.
- **Serval Project** : این پروژه یک راه‌حل شبکه مش ارائه می‌دهد که می‌تواند دستگاه‌های اندروید را به بخشی از یک شبکه غیر متمرکز تبدیل کند، امکان برقراری تماس، پیام‌رسانی و اشتراک‌گذاری فایل را بدون نیاز به اینترنت فراهم می‌کند.

ارتباطات ماهواره‌ای

برای قطع کامل اینترنت یا در مناطقی که هیچ گونه ارتباطی وجود ندارد:

- **Starlink** : استارلینک، توسط اسپیس‌ایکس اداره می‌شود و خدمات اینترنت ماهواره‌ای ارائه می‌دهد. این یکی از پیشرفته‌ترین خدمات اینترنت ماهواره‌ای است و می‌تواند در حفظ دسترسی به اینترنت در مناطق دورافتاده یا قطع‌شده حیاتی باشد.
- **Iridium یا Inmarsat** : این شبکه‌های ارتباط ماهواره‌ای جهانی، خدمات صوتی و داده‌ای ارائه می‌دهند. اگرچه گران‌تر هستند، اما در مناطقی که روش‌های ارتباط سنتی در دسترس نیستند، قابل اعتماد هستند.
- **Toosheh** : توشه یک فناوری نوآورانه است که به کاربران امکان می‌دهد محتوای دیجیتال را از طریق ماهواره دریافت کنند، بدون نیاز به دسترسی به اینترنت. این فناوری برای دور زدن محدودیت‌ها و سانسور اینترنتی بسیار مفید است.

VPN ها و ابزارهای ناشناس سازی

اگرچه VPN ها P2P نیستند، اما برای دور زدن سانسور و تأمین امنیت فعالیت های آنلاین ضروری هستند:

- **BeePass** : یک VPN ساده و امن منبع باز است که برای حفظ حریم خصوصی کاربران و عبور از سانسور اینترنت طراحی شده است.
- **Tor Browser** : ترافیک اینترنت را ناشناس می کند و به محافظت در برابر نظارت کمک می کند. به ویژه در محیط هایی که فعالیت های مرور نیاز به محرمانگی دارد، مفید است.
- **ProtonVPN** : این سرویس VPN بسیار امن، حفاظت های حریم خصوصی قوی ارائه می دهد و با ProtonMail یکپارچه شده است.
- **Psiphon** : یک ابزار دور زدن محدودیت ها که ترکیبی از SSH، VPN و فناوری های پروکسی HTTP را ارائه می دهد و در کشورهایی با سانسور شدید اینترنت بسیار استفاده می شود.
- **MahsaNet** : این VPN برای ارائه تنظیمات قابل اعتماد از طریق سرور «مهسا» طراحی شده است. هدف آن ایجاد دسترسی آسان و اقتصادی به اینترنت برای تمام کاربران است.
- **Oblivion VPN** : یک اپلیکیشن خاص VPN است که با استفاده از فناوری **Wireguard**، ارتباطات را رمزگذاری می کند و با تنظیمات ویژه خود، به دور زدن سانسور اینترنت و حفظ حریم خصوصی کاربران کمک می کند. این ابزار با ترکیب ویژگی های برتر Wireguard و دیگر فناوری های مرتبط، دسترسی امن و آسان را به اینترنت آزاد فراهم می سازد. از اینجا می توانید به اوپن سورس این وی پی ان دسترسی داشته باشید.

ابزارهای ارتباط آفلاین

در شرایطی که حتی ابزارهای P2P ممکن است غیرقابل دسترس یا محدود شوند:

- **USB Dead Drops** : این روش شامل به اشتراک گذاری اطلاعات از طریق قرار دادن USB ها در مکان های عمومی است که دیگران می توانند داده ها را از آن ها دریافت کنند. این روش که در مقایسه کمتر «تکنولوژیک» محسوب می شود برای توزیع اطلاعات در زمان قطع شدید اینترنت موثر است.
- **درایوهای USB رمزگذاری شده**: از درایوهای USB با رمزگذاری سخت افزاری برای ذخیره و انتقال امن اطلاعات حساس استفاده کنید. این ابزارها می توانند برای به اشتراک گذاشتن فایل های مهم به صورت حضوری و بدون اتکا به شبکه های دیجیتال استفاده شوند.
- **Ceno** : مرورگر (Ceno مخفف I censorship.no) یک مرورگر موبایل است که از روش های P2P برای عبور از سانسور استفاده می کند و به کاربران امکان می دهد اطلاعات وب را در مناطقی که اتصال اینترنت مختل شده است به اشتراک بگذارند.

رمزگذاری و مبهم‌سازی (Obfuscation)

رمزگذاری فرآیند تبدیل اطلاعات یا داده‌ها به کد است تا از دسترسی افراد غیرمجاز جلوگیری شود. رمزگذاری تضمین می‌کند که تنها افراد مجاز با کلید رمزگشایی صحیح می‌توانند به داده‌ها دسترسی داشته باشند و آن را بخوانند. این فرآیند برای ایمن‌سازی اطلاعات حساس مانند ایمیل‌ها، فایل‌ها، تراکنش‌های مالی و داده‌های شخصی استفاده می‌شود تا از دسترسی و درک آن توسط عوامل مخرب یا افراد غیرمجاز جلوگیری شود.

مبهم‌سازی (Obfuscation)، به نوبه خود، شامل مبهم‌سازی عمدی اطلاعات یا داده‌ها است، به طوری که حتی بدون تبدیل به قالب دیگر، فهم آن‌ها دشوار شود. برخلاف رمزگذاری، مبهم‌سازی نیازی به کلید رمزگشایی ندارد و فقط باعث می‌شود داده‌ها کمتر قابل خواندن و تفسیر باشند. هدف از مبهم‌سازی، پیچیده‌سازی داده‌ها برای جلوگیری از دسترسی غیرمجاز و دشوار کردن فهم آن است.

کاربردهای رایج رمزگذاری:

- ایمن‌سازی ایمیل‌ها برای جلوگیری از خواندن غیرمجاز.
- محافظت از فایل‌ها در برابر دسترسی غیرمجاز.
- حفظ امنیت تراکنش‌های مالی در برابر تقلب یا رهگیری.
- تضمین حریم خصوصی داده‌های شخصی در برابر سرقت یا سوءاستفاده.

کاربردهای رایج مبهم‌سازی:

- مخفی کردن منطق یک متن یا کد در نرم‌افزار برای حفاظت از مالکیت معنوی یا حریم خصوصی.
- کاهش خوانایی داده‌ها در هنگام انتقال برای جلوگیری از مشاهده تصادفی.
- افزودن پیچیدگی به فرمت‌های داده‌ها برای جلوگیری از تحلیل یا استخراج آسان.

ابزارهای رایج برای رمزگذاری و مبهم‌سازی:

- **PGP (Pretty Good Privacy)**: نرم‌افزار اولیه‌ای که GPG بر اساس آن ساخته شده است و برای ایمن‌سازی ارتباطات ایمیلی و رمزگذاری داده‌ها مورد استفاده قرار می‌گیرد.
- **VeraCrypt**: یک نرم‌افزار اوپن‌سورس محبوب برای رمزگذاری دیسک که امکان رمزگذاری فایل‌ها، پوشه‌ها یا کل درایو را فراهم می‌کند.
- **Nahoft**: یک اپلیکیشن مبهم‌سازی برای گوشی‌های اندروید و iOS است که به شما امکان می‌دهد پیام‌های خصوصی خود را به زنجیره‌ای از کلمات فارسی تبدیل کنید یا آن‌ها را در عکسی مخفی کنید و سپس از طریق هر اپلیکیشن پیام‌رسانی به طور ایمن ارسال کنید.

مخفی سازی داده ها (Data Hiding)

مخفی سازی داده ها یا استگانوگرافی به عملیاتی گفته می شود که در آن اطلاعات حساس درون فایل های غیر مشکوک مخفی می شود. برخی از ابزارهای امن و مؤثر برای مخفی سازی داده ها عبارتند از:

- **Steghide**: یک ابزار محبوب استگانوگرافی یا پنهان سازی است که به کاربران امکان می دهد داده ها را درون فایل های تصویری یا صوتی پنهان کنند. این ابزار از فرمت های مختلفی مانند BMP, JPEG, WAV و AU پشتیبانی می کند. داده های پنهان شده با استفاده از یک گذرواژه رمزگذاری می شوند، که یک لایه امنیتی اضافی فراهم می کند.
 - از چندین فرمت فایل پشتیبانی می کند.
 - از رمزگذاری قوی (AES) استفاده می کند.
 - امکان جاسازی و استخراج داده ها از فایل ها را به سادگی فراهم می کند.
- **SilentEye**: یک اپلیکیشن استگانوگرافی یا پنهان سازی دیگر است که به کاربران امکان می دهد داده ها را در فایل های تصویری و صوتی مخفی کنند. این اپلیکیشن دارای رابط کاربری گرافیکی ساده است که استفاده از آن را آسان می کند. SilentEye همچنین از رمزگذاری برای حفاظت از داده های مخفی شده پشتیبانی می کند.
 - رابط کاربری گرافیکی کاربر پسند.
 - پشتیبانی از فایل های تصویری BMP، JPG و WAV و صوتی WAV
 - رمزگذاری اختیاری برای داده های مخفی شده.
- **Crypture**: یک ابزار سبک و کاربردی برای استگانوگرافی است که داده ها را در قالب فایل های تصویری BMP مخفی می کند. این ابزار برای افرادی که به دنبال ابزاری بدون پیچیدگی های اضافه هستند، مناسب است.
 - سبک و ساده برای استفاده.
 - رمزگذاری داده های مخفی.
 - تمرکز بر روی فایل های تصویری BMP.
- **Stegano**: یک کتابخانه استگانوگرافی مبتنی بر پایتون است که می توان از آن برای مخفی سازی داده ها در تصاویر استفاده کرد. این ابزار بیشتر برای کاربرانی مناسب است که با برنامه نویسی آشنایی دارند، زیرا به دانش کدنویسی برای استفاده مؤثر نیاز دارد.
 - کتابخانه پایتون برای پیاده سازی سفارشی استگانوگرافی.
 - قابلیت ادغام در سایر برنامه ها.
 - پشتیبانی از مخفی سازی داده ها در فایل های PNG
- **Camouflage**: یک ابزار استگانوگرافی یا پنهان سازی است که فایل ها را در فایل های دیگر مانند اسناد یا تصاویر مخفی می کند. این ابزار همچنین داده های مخفی شده را فشرده و رمزگذاری می کند تا تشخیص آن ها سخت تر شود.
 - مخفی سازی فایل ها درون فایل های دیگر مانند تصاویر و اسناد.
 - فشرده سازی و رمزگذاری داده ها.
 - رابط کاربری ساده برای استفاده آسان.

- **DeepSound:** ابزاری برای مخفی سازی داده ها در فایل های صوتی است. این ابزار قابلیت جاسازی فایل های مخفی شده در آهنگ های صوتی را بدون تغییر محسوس کیفیت صدا دارد که تشخیص آن را دشوار می کند.
 - تخصص در فایل های صوتی.
 - پشتیبانی از فرمت هایی مانند WAV، FLAC و سایر فرمت ها.
 - دارای رمزگذاری AES
- **Outguess:** یک ابزار پیشرفته استگانوگرافی یا پنهان سازی است که بر روی تصاویر تمرکز دارد. این ابزار طوری طراحی شده است که داده ها را بدون ایجاد تغییرات محسوس در تصویر مخفی کند و گزینه خوبی برای کسانی است که به امنیت و عدم شناسایی بالا نیاز دارند.
 - تمرکز بر مخفی سازی داده ها در تصاویر.
 - تغییرات حداقلی در تصویر حامل.
 - پشتیبانی از فرمت های فایل JPEG و PNM
- **Tella:** یک اپلیکیشن موبایل امن است که برای فعالان، روزنامه نگاران و مدافعان حقوق بشر طراحی شده است تا اطلاعات حساس را در محیط های چالش برانگیز مستند سازی و محافظت کند. این اپلیکیشن به طور خودکار عکس ها، ویدئوها و ضبط های صوتی را رمزگذاری کرده، آن ها را از گالری معمولی گوشی مخفی می کند و به کاربران اجازه می دهد برای حفاظت بیشتر از پین یا رمز عبور استفاده کنند. Tella همچنین از جمع آوری داده به صورت آفلاین پشتیبانی می کند و با پلتفرم هایی مانند Uwazi و Kobotoolbox یکپارچه می شود. این اپلیکیشن رایگان، چند زیانه، منبع باز است و برای مقابله با سرکوب فیزیکی و دیجیتالی طراحی شده است.
 - محافظت از سرکوب فیزیکی و دیجیتالی در هنگام جمع آوری و ذخیره اطلاعات حساس.
 - محافظت از داده ها در برابر سانسور، دست کاری، رهگیری و تخریب.
 - تولید مستندات با کیفیت بالا، که می توان از آن برای تحقیقات، دفاع و عدالت انتقالی استفاده کرد.
 - رمزگذاری فایل ها: این اپلیکیشن به محض ثبت عکس ها، ویدئوها و ضبط های صوتی، آن ها را به طور خودکار رمزگذاری می کند.
 - مخفی سازی فایل ها در دستگاه: فایل های شما از گالری و فایل اکسپلورر معمولی گوشی در دسترس نیستند و فقط در داخل اپلیکیشن قابل مشاهده اند.
 - قفل گذاری فایل ها: برای حفاظت از فایل ها یک پین یا رمز عبور تنظیم کنید. وارد کردن قفل صحیح تنها راه رمزگشایی فایل های ذخیره شده در Tella است.
 - پنهان سازی ظاهر اپلیکیشن: ظاهر Tella را تغییر دهید تا برای افرادی که گوشی شما را جستجو می کنند، مخفی بماند.
 - دوربین و ضبط کننده داخلی: عکس بگیرید و ویدئوها و فایل های صوتی را مستقیماً در Tella ضبط کنید تا فایل ها بلافاصله رمزگذاری و در داخل اپلیکیشن مخفی شوند.
 - Tella با Tella Web، Uwazi، Kobotoolbox و یکپارچه می شود. پلتفرمی را انتخاب کنید که به بهترین شکل با نیازهای شما همخوانی دارد و داده ها را مستقیماً در Tella جمع آوری کنید.
 - حالت آفلاین: در مناطق با اینترنت محدود یا قطع شده، داده های خود را ذخیره کنید و در زمانی که به اتصال اینترنت مطمئن دسترسی دارید، آن ها را ارسال کنید.

حذف فراداده‌ها

در زمان قطع اینترنت، فراداده‌ها نقش مهمی دارند و اغلب به اندازه محتوای ارتباطات اهمیت دارند. فراداده‌ها اطلاعاتی درباره داده‌ها هستند، مانند اطلاعات مربوط به ارتباط افراد با یکدیگر، زمان برقراری این ارتباطات بدون فاش کردن محتوای اصلی آن ارتباطات. حتی اگر محتوا رمزگذاری شده باشد، فراداده‌ها همچنان قابل ردیابی هستند و اطلاعات ارزشمندی را فاش می‌کنند.

در ادامه اهمیت فراداده‌ها در زمان قطع اینترنت توضیح داده شده است:

• ردیابی الگوهای ارتباطی

- **پایش شبکه‌های اجتماعی:** حتی اگر محتوا به وسیله رمزگذاری پنهان شود، فراداده‌ها (مانند فرستنده، گیرنده، و زمان ارتباط) می‌توانند ارتباطات بین افراد را آشکار کنند. مقامات امنیتی و انتظامی می‌توانند از این طریق شبکه‌های فعالان، روزنامه‌نگاران یا اعضای مخالف را شناسایی کنند که می‌تواند به سرکوب هدفمند منجر شود.
- **تکرار و زمان‌بندی ارتباطات:** فراداده‌ها نشان می‌دهند که فرد چقدر ارتباط برقرار می‌کند، چه ساعاتی از روز فعال است و با چه کسانی در ارتباط است. در دوره‌های حساس سیاسی، افزایش ارتباطات بین افراد یا گروه‌های خاص می‌تواند برای مقامات هشداردهنده باشد.

• ردیابی موقعیت مکانی

- **فراداده‌های مکان‌یابی (ژئولوکیشن):** بسیاری از خدمات، به‌ویژه اپلیکیشن‌های موبایل یا مرورگرهای وب، به‌صورت خودکار اطلاعات مکانی کاربران را به عنوان بخشی از فراداده جمع‌آوری می‌کنند. حتی در شرایط محدودیت اینترنت، برخی از خدمات ممکن است همچنان قادر به ردیابی و گزارش مکان فیزیکی کاربران باشند. این مسئله در رژیم‌های سرکوبگر که به دنبال سرکوب اعتراضات و تجمعات هستند، بسیار خطرناک است.
- **شناسایی VPN و پروکسی‌ها:** حتی اگر کاربران سعی کنند با استفاده از VPN یا پروکسی‌ها از قطع اینترنت عبور کنند، فراداده‌ها می‌توانند نشان دهند که شخصی از این ابزارها استفاده می‌کند و همچنین مکان سرور VPN یا پروکسی مورد استفاده را فاش کنند. این می‌تواند افرادی را که در تلاش برای دور زدن محدودیت‌ها هستند در معرض خطر قرار دهد.

• نظارت بدون دسترسی به محتوا

- **تحلیل روابط:** در زمان قطع اینترنت، مقامات ممکن است نیازی به دیدن محتوای اصلی پیام‌ها نداشته باشند تا به اطلاعات مفید دست یابند. در این شرایط مأموران امنیتی یا ضابطین قضایی با بررسی فراداده‌ها و بررسی ارتباطات افراد، می‌توانند روابط را استنباط کنند، شبکه‌ها را ترسیم کنند و حتی اقدامات آینده را پیش‌بینی کنند. این به حکومت اجازه می‌دهد تا افراد کلیدی در جنبش‌های مدنی، سیاسی، اجتماعی را شناسایی کنند، حتی اگر محتوای ارتباطات رمزگذاری شده باشد.

- **ساختن پروفایل:** فراداده‌های جمع‌آوری شده در طول زمان می‌توانند برای ساختن پروفایلی جامع از رفتار، روابط و برنامه‌های روزمره فرد استفاده شوند. در زمان قطع اینترنت، این نوع نظارت می‌تواند برای پایش تهدیدات احتمالی یا مخالفان افزایش یابد.

• دور زدن رمزگذاری

- **محتوای رمزگذاری شده، فراداده‌های قابل مشاهده:** در حالی که رمزگذاری محتوای پیام‌ها را پنهان می‌کند، همیشه نمی‌تواند فراداده‌ها، مانند فرستنده و گیرنده پیام، طول پیام یا زمان و تکرار ارسال پیام‌ها را مخفی کند. در زمان قطع اینترنت، مقامات ممکن است تنها روش‌های ارتباطی محدودی (مانند ایمیل یا پیامک) را مجاز بدانند که در آن فراداده‌ها حتی اگر محتوا رمزگذاری شده باشد، قابل مشاهده باقی می‌مانند.

• خطرات قانونی و اجتماعی

- **جرم به واسطه ارتباط:** فراداده‌ها می‌توانند افراد را از طریق ارتباطاتشان در معرض خطر قرار دهند. حتی اگر شخصی به‌طور فعال در فعالیت‌های مخالفان درگیر نباشد، ارتباط با افرادی که تحت نظارت هستند می‌تواند او را در معرض خطر قرار دهد. به‌عنوان مثال، اگر فراداده‌ها ارتباطات مکرر با فعالان شناخته‌شده را فاش کنند، مقامات امنیتی و قضایی ممکن است آن فرد را در فعالیت‌های سیاسی یا اجتماعی مقصر بدانند.
- **چالش‌های پنهان‌سازی از نظارت:** در زمان قطع اینترنت، پنهان‌سازی فراداده‌ها بسیار دشوار است. ابزارهایی مانند VPN یا شبکه‌های ناشناس‌سازی مانند Tor کمک می‌کنند تا فراداده‌ها مبهم شوند، اما ممکن است همچنان نشانه‌هایی باقی بگذارند یا در محیط‌های تحت نظارت شدید شک برانگیز باشند.

• مسدود سازی دسترسی به منابع خارجی

- **شناسایی و مسدود سازی ترافیک:** حتی اگر کاربران سعی کنند از طریق ابزارهای ارتباطی خارجی (مانند VPN، پروکسی‌ها، یا اپلیکیشن‌های پیام‌رسان رمزگذاری شده) محدودیت‌های قطع اینترنت را دور بزنند، فراداده‌ها می‌توانند این تلاش‌ها را آشکار کنند. مقامات می‌توانند با تحلیل الگوهای فراداده و شناسایی ابزارهای مورد استفاده، این روش‌ها را مسدود کنند.

حفاظت از فراداده‌ها در زمان قطع اینترنت

- در حالی که رمزگذاری محتوای پیام‌ها بسیار ضروری است، روش‌هایی نیز برای حفاظت از فراداده‌ها وجود دارد:
- **استفاده از شبکه‌های Tor یا I2P:** این ابزارهای ناشناس‌سازی با مسیریابی ترافیک از طریق چندین گره، فراداده‌ها را مبهم کرده و ردیابی مبدا یا مقصد ارتباط را برای مقامات دشوار می‌کنند.
- **VPN‌ها و پروکسی‌ها:** با اینکه کامل نیستند، VPN‌ها می‌توانند برخی از انواع فراداده‌ها مانند آدرس IP کاربر را از طریق مسیریابی ترافیک از سرورهای خارجی پنهان کنند. با این حال، خود استفاده از VPN نیز ممکن است قابل ردیابی باشد.
- **تاخیر عمدی در ارسال پیام‌ها:** ابزارهایی مانند «شبکه‌های میکس» تأخیرهایی به پیام‌ها اضافه می‌کنند تا فراداده‌های زمانی را مبهم کرده و ارتباط بین فرستنده و گیرنده را دشوار کنند.

در شرایط قطع اینترنت، فراداده‌ها می‌توانند نقشه دقیقی از اینکه چه کسی با چه کسانی، چه زمانی و از کجا ارتباط دارد، حتی بدون دسترسی به محتوای پیام‌ها، به مقامات ارائه دهند. بنابراین، حفاظت از فراداده‌ها به اندازه ایمن‌سازی محتوای ارتباطات اهمیت دارد، به‌ویژه برای افرادی که در فعالیت‌های حساسی مانند اعتراضات، روزنامه‌نگاری یا دفاع از حقوق بشر مشغول هستند.

ابزارهای ساده و کاربردی برای حفاظت از فراداده‌ها:

• [MAT2](#) (ابزار ناشناس‌سازی فراداده‌ها)

- **کارکرد:** MAT2 یک ابزار رایگان و ساده برای حذف فراداده از اسناد، تصاویر، فایل‌های PDF و انواع دیگر فایل‌ها است. این ابزار از فرمت‌های گسترده‌ای پشتیبانی کرده و فراداده‌های حساس مانند نام نویسنده، اطلاعات مکان و تاریخچه تغییرات را حذف می‌کند.
- **نحوه استفاده:** دارای رابط کاربری گرافیکی است که با قابلیت کشیدن و رها کردن فایل‌ها به کاربران غیر فنی کمک می‌کند فایل‌های خود را پیش از اشتراک‌گذاری پاک‌سازی کنند.
- **امکان استفاده:** در سیستم‌عامل‌های لینوکس، قابل استفاده از طریق خط فرمان و در برخی توزیع‌های لینوکس نسخه‌های کاربر پسند موجود است.

• [ExifTool](#) (برای تصاویر و ویدیوها)

- **کارکرد:** ExifTool ابزاری قدرتمند برای حذف فراداده‌ها، به‌ویژه از فایل‌های تصویری و ویدیویی است که ممکن است داده‌های GPS، اطلاعات دوربین یا زمان‌بندی‌ها را شامل شود.
- **نحوه استفاده:** به‌طور پیش‌فرض فنی‌تر است، اما رابط‌های کاربرپسند مانند "ExifCleaner" برای کاربران غیر فنی فرآیند را ساده کرده و امکان کشیدن و رها کردن فایل‌ها برای حذف فراداده‌ها را فراهم می‌کنند.
- **امکان استفاده:** قابل استفاده در سیستم‌عامل‌های ویندوز، macOS و لینوکس.

• [VLC Media Player](#) (برای فراداده‌های ویدیوها)

- **کارکرد:** VLC که یک پخش‌کننده چندرسانه‌ای رایج است و ابزارهای داخلی برای ویرایش یا حذف فراداده‌ها از فایل‌های ویدیویی را دارد. کاربران می‌توانند به‌سادگی یک ویدیو را باز کرده، فراداده‌ها را ویرایش یا به‌کلی حذف کنند.
- **نحوه استفاده:** ویدیو را باز کرده، به قسمت «ابزارها» < «اطلاعات رسانه» بروید و فیلدهای فراداده را به‌صورت دستی ویرایش یا پاک کنید. این روش برای کاربران غیر فنی ساده است.
- **امکان استفاده:** برای ویندوز، macOS و لینوکس.

• [AnonAddy](#) (برای فراداده‌های ایمیل)

- **کارکرد:** AnonAddy یک سرویس ساده برای ارسال و دریافت ایمیل به‌صورت ناشناس است که آدرس ایمیل واقعی شما را مخفی کرده و فراداده‌هایی مانند آدرس IP را حذف می‌کند.
- **نحوه استفاده:** کاربران می‌توانند از طریق ایجاد نام‌های مستعار ناشناس برای ایمیل خود، ایمیل‌ها را بدون نمایش اطلاعات شخصی یا فراداده ارسال و دریافت کنند.
- **امکان استفاده:** با هر کلاینت ایمیلی سازگار است و از طریق مرورگر وب قابل دسترسی است.

- **OnionShare** (برای اشتراک گذاری فایل به صورت ناشناس)
 - کارکرد: OnionShare به کاربران امکان می‌دهد فایل‌ها را به صورت امن و ناشناس با استفاده از شبکه Tor به اشتراک بگذارند و فراداده‌های مرتبط با فرآیند اشتراک گذاری را پنهان کند.
 - نحوه استفاده: کاربران غیر فنی می‌توانند OnionShare را نصب کرده، فایل‌های خود را به سادگی کشیده و رها کرده و یک لینک امن دریافت کنند که می‌توانند به گیرنده ارسال کنند.
 - امکان استفاده: برای ویندوز، macOS و لینوکس.
- **Tor Browser** (برای وب گردی و ارتباطات)
 - کارکرد: مرورگر Tor ترافیک اینترنتی کاربران را از چندین گره عبور داده و فراداده‌هایی مانند آدرس IP و عادات‌های مرور را مخفی می‌کند. این یکی از ساده‌ترین ابزارها برای کاربران غیر فنی است که از فعالیت‌های آنلاین خود محافظت کنند.
 - نحوه استفاده: مرورگر Tor را دانلود کرده و مانند یک مرورگر معمولی از آن استفاده کنید. این مرورگر به طور خودکار ترافیک شما را ناشناس می‌کند.
 - امکان استفاده: برای ویندوز، macOS، لینوکس و اندروید.
- **Simple PDF Metadata Remover** (حذف فراداده PDF)
 - کارکرد: این ابزار به صورت خاص برای حذف فراداده از PDFها طراحی شده و اطلاعاتی مانند نام نویسنده، تاریخ ایجاد سند و تاریخچه تغییرات را پاک می‌کند.
 - نحوه استفاده: کاربران می‌توانند فایل PDF خود را به سادگی کشیده و رها کرده و با یک کلیک فراداده‌ها را حذف کنند.
 - در دسترس بودن: به عنوان یک برنامه ساده برای ویندوز.
- **BleachBit** (برای پاک سازی کلی فایل‌ها)
 - کارکرد: BleachBit ابزاری کاربرپسند است که به حذف فراداده‌ها از انواع مختلف فایل‌ها و پاک سازی داده‌های غیرضروری از رایانه کمک می‌کند تا حریم خصوصی کاربران حفظ شود.
 - نحوه استفاده: رابط کاربری ساده‌ای ارائه می‌دهد که کاربران می‌توانند نوع فایل‌هایی را که می‌خواهند پاک سازی کنند (مانند تاریخچه مرورگر، فراداده‌ها و بیشتر) انتخاب کرده و با یک کلیک پاک سازی را انجام دهند.
 - امکان استفاده: برای ویندوز و لینوکس.
- **اپلیکیشن‌های حذف فراداده عکس (برای گوشی‌های هوشمند)**
 - کارکرد: این اپلیکیشن‌ها برای حذف فراداده‌ها از عکس‌های گوشی‌های هوشمند طراحی شده‌اند، مانند داده‌های EXIF که اطلاعات مکان و دوربین را شامل می‌شوند.
 - نحوه استفاده: کاربران فقط نیاز به آپلود عکس دارند و اپلیکیشن به طور خودکار فراداده‌ها را حذف می‌کند.
- **سیستم عامل Tails (برای حفظ کامل حریم خصوصی)**
 - کارکرد: Tails یک سیستم عامل متمرکز بر حریم خصوصی است که از طریق USB اجرا می‌شود و تمام فعالیت‌ها را ناشناس می‌کند. این سیستم عامل به صورت پیش فرض با ابزارهایی مانند Tor، ارتباطات رمزگذاری شده و حذف فراداده برای فایل‌ها بارگذاری شده است.

○ **نحوه استفاده:** نصب Tails ممکن است به دانش فنی مختصری نیاز داشته باشد، اما پس از راه اندازی، تمام ابزارها ساده و برای حریم خصوصی از پیش تنظیم شده اند، که آن را برای کاربران غیر فنی که به حفاظت جامع نیاز دارند، ایده آل می کند.

○ **امکان استفاده:** به صورت رایگان در دسترس است، اما به یک فلش USB برای نصب و اجرا نیاز دارد. این ابزارها برای کاربران غیر فنی، روش های ساده و موثری برای حذف یا پنهان کردن فراداده ها ارائه می دهند و با رابط های کشیدن و رها کردن، پاک سازی با یک کلیک، و ابزارهای ناشناس سازی مانند Tor یا Tails پیچیدگی های فرآیند را به صورت خودکار انجام می دهند.

سناریوهای عملی و قابل اجرا

در اینجا به بررسی چهار سناریوی واقعی خواهیم پرداخت. در این سناریوها، نه تنها روش های مورد استفاده کاربران تحلیل خواهند شد، بلکه ریسک های امنیتی نیز بررسی شده و راه حل هایی برای کاهش این ریسک ها ارائه خواهد شد.

سناریوی اول: قطع کامل اینترنت و استفاده از ابزارهای ارتباطی داخلی

در زمان قطع اینترنت، من در تهران بودم در حالی که همسر من که شهروند ایالات متحده است در آنجا حضور داشت. برای چند روز هیچ راهی برای ارتباط با او نداشتم تا اینکه متوجه شدم می توانم از طریق خدمات ایمیل مبتنی بر اینترنت ملی با دامنه ir. ایمیل هایی به جیمیل ارسال و دریافت کنم. پس از چند روز سکوت، بالاخره توانستیم ارتباط برقرار کنیم، اما به دلیل نگرانی از اینکه ایمیل های ir. خوانده شوند، مکالمات ما بسیار رسمی بود. سعی می کردیم به صورت مبهم و غیرمستقیم صحبت کنیم، نگران از اینکه کسی ممکن است نظارت کند.

راه حل: حتی در زمان قطع اینترنت، برخی خدمات اینترنت ملی ممکن است فعال باقی بمانند (مانند ایمیل های با دامنه ir.). در این شرایط، می توان از [رمزگذاری GPG](#) بر روی این پلتفرم ها استفاده کرد تا محتوا برای افراد ثالث به راحتی قابل خواندن نباشد. همچنین می توان یک فایل یا پیام متنی رمزگذاری شده ایجاد کرده و از طریق کانال های دیگر مانند پیام رسان ها یا حتی پیامک ارسال کرد.

برنامه ریزی پیشگیرانه: قبل از قطع اینترنت، فرد و همسرش می توانند رمزگذاری GPG را برای ایمیل های خود تنظیم کنند. GPG امکان رمزگذاری پیام ها را فراهم می کند، به طوری که تنها گیرنده مورد نظر قادر به خواندن آن ها باشد. این زوج می توانند کلیدهای عمومی GPG خود را از قبل رد و بدل کنند تا حتی در پلتفرم های تحت نظارت نیز بتوانند به صورت ایمن ارتباط برقرار کنند.

سناریوی دوم: قطع شبکه داده موبایل

در زمان قطع اینترنت در شهری بزرگ مانند تهران، مقامات با هدف اختلال در اینترنت موبایل (3G/4G) به‌ویژه در مناطقی مانند پارک لاله که اعتراضات در جریان بود، شبکه‌های مخابراتی (BTS) را هدف قرار دادند. همه سیم‌کارت‌ها از دسترسی به اینترنت، از جمله خدمات LTE، قطع شدند. با این حال، در حالی که اینترنت موبایل قطع شده بود، اینترنت ثابت خانگی (ADSL/TD-LTE) همچنان فعال بود.

با بهره‌گیری از این فرصت، با استفاده از VPN از طریق گوشی به شبکه اینترنت خانگی‌ام متصل شدم. از طریق ایجاد اتصال امن به وای‌فای خانگی‌ام از طریق VPN، توانستم قطع اینترنت موبایل را دور زده و به اینترنت دسترسی پیدا کنم. پس از اتصال، گوشی خود را به نقطه اتصال تبدیل کردم و امکان دسترسی به اینترنت را برای دیگران در اطرافم نیز فراهم کردم. در حالی که بسیاری از افراد دسترسی به اینترنت نداشتند من و اطرافیانم دسترسی کامل به اینترنت داشتیم.

یک هشدار نیز منتشر شده بود که به دلیل احتمال ردیابی، از آوردن تلفن همراه به محل اعتراضات خودداری کنید؛ اما راه‌حل من این امکان را فراهم کرد که با استفاده از شبکه امن خانگی‌ام، دسترسی به اینترنت را به روشی امن‌تر برای دیگران فراهم کنم.

راه‌حل: این روش بر این اساس استوار است که در حالی که شبکه‌های موبایل (BTS) قطع می‌شوند، خدمات اینترنت ثابت مانند ADSL یا TD-LTE ممکن است همچنان فعال بمانند. با اتصال به اینترنت ثابت از طریق VPN از دستگاه موبایل، می‌توان دسترسی به اینترنت را بازیابی کرد و با تبدیل گوشی به نقطه اتصال، این اتصال را با دیگران به اشتراک گذاشت.

اجرای این راه‌حل:

- استفاده از اینترنت ثابت: اگر اینترنت ثابت خانگی‌تان هنوز فعال است، از آن برای دسترسی به اینترنت جهانی استفاده کنید.
- اتصال از طریق VPN: یک VPN بر روی گوشی نصب و تنظیم کنید تا حتی در زمان قطع اینترنت موبایل، بتوانید به‌صورت ایمن به شبکه خانگی متصل شوید.
- ایجاد نقطه اتصال: پس از اتصال از طریق VPN، قابلیت نقطه اتصال گوشی را فعال کرده و اتصال اینترنت را با دیگران به اشتراک بگذارید.

این راه‌حل دسترسی مستمر به پلتفرم‌های آنلاین را در زمان اختلال شبکه‌های موبایل تضمین می‌کند و به شما امکان می‌دهد تا در لحظه متصل بمانید و به دیگران کمک کنید.

برنامه‌ریزی پیشگیرانه: جهت آماده‌سازی برای چنین شرایطی، ضروری است که پیش از قطع اینترنت، گام‌های مشخصی برداشته شود. در ادامه، نحوه برنامه‌ریزی را مشاهده می‌کنید:

تهیه ابزارهای لازم:

- سرویس VPN: یک سرویس VPN نصب کنید که امکان اتصال از راه دور به شبکه اینترنت خانگی را فراهم کند. اطمینان حاصل کنید که این سرویس بر روی گوشی و سایر دستگاه‌های شما نصب و تنظیم شده است.

- **اتصال اینترنت ثابت:** مطمئن شوید که اتصال اینترنت خانگی پایدار و قابل اعتمادی مانند TD-LTE یا ADSL دارید که می‌تواند در مواقع قطع شبکه موبایل استفاده شود.
- **قابلیت نقطه اتصال موبایل:** با قابلیت نقطه اتصال (هات اسپات) گوشی آشنا شوید و مطمئن شوید که این قابلیت فعال و تنظیم شده است.

هماهنگی با دیگران:

- به دوستان و خانواده اطلاع دهید که چه تنظیماتی انجام داده‌اید تا در صورت قطعی اینترنت، بتوانند به نقطه اتصال موبایل شما متصل شوند.
- آن‌ها را تشویق کنید تا تنظیمات مشابهی را برای پشتیبانی و کاهش بار راه‌اندازی کنند.

تهدیدهای احتمالی:

- **نظارت:** حتی در صورت استفاده از VPN برای رمزگذاری اتصال، مقامات همچنان ممکن است الگوهای ترافیک یا فراداده‌ها را پایش کنند، به‌ویژه اگر کنترل ISP‌های محلی را در اختیار داشته باشند. استفاده از ابزارهای رمزگذاری مانند VPN یا Tor برای محافظت از داده‌ها ضروری است.
- **امنیت فیزیکی:** حمل موبایل با نقطه اتصال روشن ممکن است توجه را جلب کند، به‌ویژه اگر دسترسی شما به اینترنت مشهود باشد در حالی که دیگران قطع ارتباط دارند. مراقب باشید که اتصال خود را در کجا استفاده می‌کنید و از جلب توجه در مناطق با امنیت بالا یا اعتراضات خودداری کنید.
- **اختلال در خدمات:** با وجود اینکه خدمات اینترنت ثابت مانند TD-LTE یا ADSL ممکن است فعال بمانند، احتمال قطع آن‌ها نیز وجود دارد. هیچ تضمینی وجود ندارد که این اتصالات در طول قطعی‌های طولانی مدت نیز پایدار باقی بمانند.
- **تخلیه باتری:** استفاده از گوشی به‌عنوان نقطه اتصال می‌تواند باتری آن را به سرعت تخلیه کند، به‌ویژه در استفاده طولانی مدت. مطمئن شوید که شارژرهای قابل حمل یا منابع تغذیه در دسترس دارید تا اتصال را برای مدت زمان طولانی‌تر حفظ کنید.

سناریوی سوم: قطع تقریباً کامل اینترنت و استفاده از زیرساخت‌های داخلی و رومینگ

در پاسخ به افزایش قطعی‌های اینترنت، گروهی به نام «ارتش مخفی» ایجاد کردیم تا راهی برای دور زدن این محدودیت‌ها و حفظ دسترسی به اینترنت پیدا کنیم. متوجه شدیم که می‌توانیم از سیم‌کارت‌های خارجی کشورهای مانند ترکیه و امارات، همچنین مراکز داده داخلی در ایران برای دسترسی به اینترنت استفاده کنیم.

استراتژی اصلی ما این بود که کاربران را از طریق VPN به سیم‌کارت‌های خارجی که از خدمات رومینگ در داخل ایران استفاده می‌کردند متصل کنیم. با این روش، ترافیک کاربران به شبکه‌های بین‌المللی منتقل شد و حتی در زمانی که شبکه‌های محلی قطع بودند، دسترسی به اینترنت را حفظ کردیم.

زمانی که خدمات رومینگ نیز مسدود شد، به روش دیگری سازگار شدیم و کاربران را به مراکز داده داخلی متصل کردیم. از طریق اتصال VPN، کاربران به این مراکز داده داخلی که هنوز به اینترنت جهانی متصل بودند دسترسی پیدا کردند. به این ترتیب، حتی در شرایط قطعی شدید، توانستیم ارتباطات و کانال‌های حیاتی اطلاعات را حفظ کنیم.

راه‌حل: راه‌حل در این سناریو بر دو استراتژی کلیدی متکی بود: استفاده از سیم‌کارت‌های خارجی با خدمات رومینگ و مراکز داده داخلی. این روش‌ها به کاربران امکان دادند که علی‌رغم اختلالات شبکه‌های محلی، به اینترنت متصل بمانند.

نحوه عملکرد:

- استفاده از سیم‌کارت‌های خارجی برای رومینگ: ما به کاربران دسترسی به سیم‌کارت‌های خارجی (مانند ترکیه و امارات) که همچنان خدمات رومینگ فعال در داخل ایران داشتند، ارائه کردیم. با اتصال به این سیم‌کارت‌ها از طریق VPN، کاربران توانستند محدودیت‌های اینترنتی ایران را دور بزنند و به خدمات اینترنت بین‌المللی دسترسی پیدا کنند.
- اتصال به مراکز داده داخلی: هنگامی که مقامات خدمات رومینگ را مسدود کردند، استراتژی خود را به مراکز داده داخلی تغییر دادیم. با مسیریابی ترافیک VPN از طریق این مراکز داده که به اینترنت جهانی متصل بودند، کاربران توانستند حتی در زمان قطعی گسترده اینترنت به خدمات آنلاین دسترسی داشته باشند.
- هر دو روش به ما امکان دادند تا در لحظات بحرانی به کاربران دسترسی به اینترنت ارائه کنیم، به‌طوری که ارتباطات، به‌روزرسانی‌ها و تبادل اطلاعات علی‌رغم تلاش‌های دولت برای ایزوله‌سازی جامعه همچنان امکان‌پذیر باقی بماند.
- برنامه‌ریزی پیشگیرانه: برای اطمینان از اینکه این روش در قطعی‌های اینترنت آینده به‌خوبی کار کند، ضروری است که از قبل برنامه‌ریزی و آماده‌سازی انجام شود. در ادامه مراحل آماده‌سازی ذکر شده است:

• تهیه سیم‌کارت‌های خارجی

- اطمینان حاصل کنید که شما یا افراد مورد اعتماد به سیم‌کارت‌های خارجی از کشورهایی مانند ترکیه یا امارات دسترسی دارند. این سیم‌کارت‌ها را از قبل تست کنید تا مطمئن شوید می‌توانند از طریق رومینگ در ایران متصل شوند.
- برای توزیع این سیم‌کارت‌ها به کاربران مورد اعتماد در مواقع قطعی گسترده اینترنت، یک برنامه پشتیبان داشته باشید.

• راه‌اندازی زیرساخت VPN

- سرورهای VPN را راه‌اندازی و پیکربندی کنید تا بتوانند ترافیک را از طریق سیم‌کارت‌های خارجی یا مراکز داده داخلی مسیریابی کنند. اطمینان حاصل کنید که VPN با این سیم‌کارت‌ها تست شده و می‌تواند اتصالات امن برقرار کند.
- چندین پیکربندی VPN آماده داشته باشید تا در صورت مسدود شدن یک سرور یا روش، گزینه‌های دیگری در دسترس باشد.

• ایجاد ارتباط با مراکز داده داخلی

- مراکز داده داخلی را شناسایی کنید و ارتباطات امنی با آنها برقرار کنید که حتی در زمان قطعی‌های جزئی همچنان به اینترنت جهانی دسترسی دارند. در صورت امکان، با افراد مورد اعتماد در این مراکز داده ارتباط برقرار کنید تا اتصال به اینترنت حفظ شود.
- اطمینان حاصل کنید که VPN می‌تواند ترافیک را به‌راحتی از طریق این مراکز داده مسیریابی کند اگر خدمات رومینگ قطع شدند.

• تست منظم سیستم‌های پشتیبان

- به‌طور منظم کل تنظیمات را تست کنید، از اتصال VPN گرفته تا عملکرد سیم‌کارت‌های خارجی و مراکز داده. اطمینان حاصل کنید که کاربران می‌دانند در مواقع نیاز چگونه به این سیستم‌ها متصل شوند.
- یک کانال ارتباطی امن و خصوصی ایجاد کنید تا به کاربران آموزش دهید چگونه به VPN متصل شده و در زمان قطعی اینترنت دسترسی را حفظ کنند.

تهدیدات احتمالی: در حالی که این روش می‌تواند دسترسی به اینترنت را در شرایط قطعی شدید فراهم کند، خطراتی نیز به همراه دارد:

- **نظارت و شناسایی:** مقامات ممکن است ترافیک سیم‌کارت‌های خارجی یا مراکز داده داخلی را پایش کنند، به‌ویژه اگر مشکوک شوند که افراد از این روش‌ها برای دور زدن قطعی اینترنت استفاده می‌کنند. استفاده از رمزگذاری (مانند Tor، VPN و غیره) ضروری است تا خطر نظارت و شناسایی به حداقل برسد.
- **امنیت فیزیکی:** در اختیار داشتن سیم‌کارت‌های خارجی یا دسترسی به مراکز داده داخلی ممکن است در مناطق با امنیت بالا یا تحت نظارت دولت شک‌برانگیز باشد. اطمینان حاصل کنید که افراد درگیر از خطرات احتمالی آگاه بوده و می‌دانند چگونه در چنین شرایطی رفتار کنند.
- **قطع مراکز داده:** اگر دولت تشخیص دهد که از مراکز داده داخلی برای دور زدن محدودیت‌ها استفاده می‌شود، ممکن است دسترسی به این مراکز را نیز مسدود کند. داشتن چندین سرور VPN یا روش‌های جایگزین ضروری است تا اتصال امن حفظ شود.
- **ازدحام روی سیم‌کارت‌های خارجی:** اگر تعداد زیادی کاربر به تعداد محدودی سیم‌کارت خارجی متصل شوند، شبکه ممکن است دچار ازدحام شده و باعث کاهش عملکرد یا ایجاد مشکلات اتصال شود. داشتن سیم‌کارت‌ها و سرورهای VPN متعدد برای توزیع بار شبکه ضروری است.

سناریوی چهارم: استفاده از پلتفرم‌های بازی و کسب‌وکار برای ارتباطات

پس از حادثه اسقاط هواپیمای اوکراینی و محدودیت‌های اینترنت در سراسر کشور، به روش‌های قدیمی ارتباطی مانند فکس و پیامک برای اطلاع‌رسانی درباره برگزاری نمایشگاه برگشتیم، این وضعیت یادآور اوایل دهه ۲۰۰۰ بود. اینترنت دیگر هرگز مثل قبل نبود. ما مجبور شدیم به سیستم‌های ارتباطی منسوخ مانند ارسال نامه با پیک موتوری تکیه کنیم. در زندگی شخصی من، قطع اینترنت ارتباطم را با دنیای بیرون کاملاً قطع کرد. احساس می‌کردم در جزیره‌ای گیر افتاده‌ام و هیچ راهی برای ارتباط با جهان بیرون یا فرار ندارم. گرچه این قطع ارتباط لزوماً زندگی روزمره را مختل نمی‌کرد، اما احساس ناامنی شدیدی داشت. برای دسترسی به اخبار مجبور شدیم به سایت «[پیوندها](#)»، صفحه سانسور اینترنت ایران، سر بزنیم. بدون دسترسی به تلویزیون یا ماهواره، تلاش می‌کردیم از منابع خبری داخلی حقیقت را کنار هم بگذاریم. به دلیل نگرانی از پروتکل‌های مربوط به حفاظت احريم خصوصي، به اپلیکیشن‌های داخلی اعتماد نداشتیم. از سوی دیگر مطالبی در رابطه با اینترنت ماهواره‌ای شنیده بودم اما قیمت آن خیلی بالا بود. در نتیجه، بسیاری از ما به VPN‌ها متوسل شدیم تا سعی کنیم دوباره به اینترنت جهانی دسترسی پیدا کنیم. گاهی اوقات اتاق‌های خبر رسانه‌ها «امتیازهای» اینترنت محدود و بسیار کمی ارائه می‌دادند که عمدتاً برای عکاسان بود و حس می‌کردیم که بسیار تحت کنترل و دستکاری شده است.

پس از اعتراضاتی که با جان باختن مهسا آغاز شد، اینترنت در برخی مناطق قطع شد تا ارتباطات مختل و از سازماندهی جلوگیری شود. اما ما راه‌های جایگزینی برای ارتباط پیدا کردیم، از جمله استفاده از پلتفرم‌های بازی و اپلیکیشن‌های داخلی مانند **دیوار** که احتمال کمتری برای نظارت بر آنها وجود داشت.

در سپتامبر ۲۰۲۲، این وضعیت تشدید شد. دیگر برای جلوگیری از گسترش نظارت دولت خیلی دیر شده بود و مهم‌ترین اولویت این بود که فعالیت‌های مان جان دیگران را به خطر نیندازد. گروهی در محله ما در اکباتان یک تجمع اعتراضی سازماندهی کرده بودند، اما زمانی که به آنجا رسیدیم، منطقه پر از نیروهای بسیجی بود.

ما کدهایی برای ارتباط ایمن ایجاد کرده بودیم. ابتدا ساکت می‌ماندیم و فاصله می‌گرفتیم تا شرایط را بسنجیم. همچنین کانال‌های پشتیبان ارتباطی داشتیم، از جمله گروه خاصی در تلگرام با اعضای مشترک که زبان و کدهای خاصی را برای انتقال اطلاعات می‌دانستند. بسیاری از این افراد طراح بازی بودند و بازی‌هایی ایجاد کرده بودند که به‌طور مخفیانه برای سازماندهی استفاده می‌شد؛ در واقع کسی بازی نمی‌کرد، بلکه این پلتفرم‌ها به‌عنوان ابزاری برای ارتباطات به کار می‌رفتند.

به عنوان عکاس، همواره نگران حفاظت از خود و کارم بودم و به روش‌های سنتی بازگشتم تا امنیت بیشتری داشته باشم. در دو یا سه روز اول اعتراضات، من و بسیاری از همکارانم، دوربین‌هایمان را به خیابان بردیم تا وقایع را مستند کنیم. اما وقتی دستگیری‌ها و ضبط دوربین‌ها شروع شدند، استفاده از تلفن همراه را متوقف کردم. به جای آن، از یک دوربین سونی قدیمی بدون لنز و با یک کارت SD کوچک استفاده کردم که به اینترنت متصل نبود. زمانی که در نهایت کارت SD را از بین بردم، هیچ اثری از کارهایمان باقی نماند. همواره در قاب‌بندی عکس‌ها مراقب بودم تا چهره افراد را محو کنم و هویت آن‌ها را حفظ کنم.

راه‌حل: برای کاهش تأثیرات قطع اینترنت، به ویژه برای افرادی که در حوزه‌های حساس یا خلاقانه و هنری فعالیت می‌کنند، یک راه‌حل چند لایه لازم است:

- **پلتفرم‌های ارتباطی جایگزین:** در زمان اعتراضات، افراد می‌توانند از پلتفرم‌های بازی یا اپلیکیشن‌های داخلی مانند دیوار به‌عنوان کانال‌های ارتباطی مخفی استفاده کنند. از آنجا که تمام این ارتباطات به صورت متنی انجام می‌شود، کاربران باید آدرس IP خود را پنهان کرده و تمام ارتباطات را رمزگذاری کنند.
 - **ذخیره و انتقال داده‌های رمزگذاری‌شده:** استفاده از ابزارهای رمزگذاری قوی مانند GPG برای حفاظت از ارتباطات و داده‌ها، به ویژه برای روزنامه‌نگاران و هنرمندان، ضروری است. علاوه بر این، آن‌ها باید به‌طور منظم از کارهای خود نسخه‌های پشتیبان تهیه و به‌صورت آفلاین و رمزگذاری‌شده (مانند USB یا SSD) ذخیره کنند. این نسخه‌های پشتیبان می‌توانند از طریق سرویس‌های ابری یا راهکارهای ذخیره‌سازی غیرمتمرکز مانند IPFS در خارج از کشور نیز نگهداری شوند.
 - **پلتفرم‌های غیرمتمرکز برای به اشتراک‌گذاری آثار و محتوا:** هنرمندان باید به پلتفرم‌های مبتنی بر بلاکچین برای نمایش آثار خود توجه کنند. فناوری‌های غیرمتمرکز مانند NFTها می‌توانند به هنرمندان این امکان را بدهند که حتی در صورت مسدود شدن پلتفرم‌های مرکزی مانند اینستاگرام، آثار خود را به صورت جهانی به اشتراک بگذارند.
- برنامه‌ریزی پیشگیرانه:** برای آماده‌سازی جهت قطعی‌های احتمالی اینترنت در آینده، افراد و سازمان‌ها باید از پیش برنامه‌ریزی کنند:

- **شبکه‌های مش (Mesh Networks):** ایجاد شبکه‌های محلی مش که به دستگاه‌های الکترونیکی امکان اتصال مستقیم بدون نیاز به اینترنت گسترده را می‌دهد، ضروری است. این شبکه‌ها برای حفظ ارتباطات در زمان قطعی‌های طولانی مدت، به‌ویژه در مناطق شهری متراکم، بسیار کاربردی خواهند بود.
 - **پشتیبان‌گیری و مدیریت داده‌های آفلاین:** پشتیبان‌گیری منظم از داده‌ها در مکان‌های امن و آفلاین اطمینان می‌دهد که کارها و ارتباطات حتی در زمان قطعی‌ها قابل دسترسی باقی می‌مانند. استفاده از خدماتی مانند IPFS برای ذخیره‌سازی غیرمتمرکز یا فضای ابری امن بین‌المللی می‌تواند یک لایه حفاظتی برای داده‌های حساس فراهم کند.
 - **آموزش سواد دیجیتال و امنیت:** آموزش روش‌های ارتباط امن به هنرمندان، فعالان و دیگر گروه‌های آسیب‌پذیر، از جمله استفاده از VPN، ابزارهای رمزگذاری و سیستم‌های پشتیبان‌گیری آفلاین، به آن‌ها کمک می‌کند که در مواجهه با قطعی اینترنت آمادگی بیشتری داشته باشند.
- با پذیرش این راه‌حل‌ها و اجرای اقدامات پیشگیرانه، افراد، کسب‌وکارها و هنرمندان می‌توانند حتی در زمان قطع اینترنت، کار خود را با امنیت و اطمینان بیشتری ادامه دهند. این امر به محافظت از ارتباطات حیاتی، تداوم کارهای خلاقانه، هنری و حفظ آزادی بیان و سازماندهی کمک می‌کند.

بازی قطع اینترنت

بازی «قطع اینترنت» با دقت طراحی شده است تا تجربه‌ای جذاب و آموزشی پیرامون موضوع قطع اینترنت ارائه دهد. هدف اصلی آن، آشنا کردن شرکت‌کنندگان با تکنیک‌های مختلفی است که برای مختل کردن دسترسی به اینترنت به کار می‌روند و همچنین شامل راهبردهایی برای مقابله با این محدودیت‌ها است. این بازی با هدف برجسته‌سازی موضوع مهم سانسور اینترنت ساخته شده است و به بررسی انگیزه‌های پشت این قطعی‌ها و تأثیرات آن‌ها بر حقوق بشر می‌پردازد. با استفاده از این بازی با قابلیت مشارکت فعال یا گیم‌پلی تعاملی، افراد و سازمان‌ها می‌توانند دانش قابل توجهی در رابطه با روش‌های دولت‌ها برای مسدود کردن دسترسی به اینترنت پیدا کنند و راه‌های مؤثری برای حفاظت از آزادی دیجیتال بیاموزند. این بازی در گردهمایی‌های حضوری و آنلاین قابل استفاده است و به‌عنوان یک ابزار چندکاره برای گروه‌های متنوع عمل می‌کند و شامل دستورالعمل‌های دقیق برای تسهیل‌گران، دینامیک‌های بازی و منابعی مانند نقشه‌ها و کارت‌ها برای افزایش کیفیت تجربه‌ی بازی است. در یک جلسه ۱۲۰ دقیقه‌ای، بازیکنان به جنبه‌های فنی قطع اینترنت می‌پردازند، با سناریوهای واقعی مواجه می‌شوند و با استفاده از کارت‌های «دور زدن» روش‌های مختلف برای عبور از محدودیت‌ها را بررسی می‌کنند. با بهره‌گیری از مجوز اشتراک‌گذاری آزاد (creative commons license)، این بازی به کاربران اجازه می‌دهد محتوا را متناسب با نیازهای خود تغییر دهند، درک عمیق‌تری از زیرساخت اینترنت به دست آورند و توانایی خود برای مقابله و مقاومت در برابر قطع اینترنت را تقویت کنند.

محتویات فایل‌های بازی:

- **راهنمای بازی:** شامل دستورالعمل‌هایی برای کمک به تسهیل‌گران در سازماندهی جلسات آموزشی؛ هم به صورت آنلاین و هم به صورت حضوری.
 - **۱۳ سناریوی مسدودسازی:** برای انتخاب سناریوهای مرتبط با مخاطب و اهداف مورد نظر.
 - **ارائه‌ها و تصاویر قابل ویرایش:** برای تطبیق مطالب با نیازها و ویژگی‌های مخاطب.
- توجه داشته باشید که این بازی برای یادگیری شخصی درباره قطع اینترنت طراحی نشده است و نیازمند حضور تسهیل‌گر و تعامل با دیگران است.