سرفصل ها

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 سیسی سیاسی، مانند آنچه در ایران دیده شده است، صورت می‌گیرد.

قطع اینترنت می‌توانند به‌صورت کامل باشند، که در آن دسترسی به تمامی بخش‌های شبکه‌ها قطع می‌شود، یا به‌صورت 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 به‌طور 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 بینجامند.

قطع اینترنت به طور فزاینده‌ای به‌عنوان ابزاری برای سرکوب حکومت مورد استفاده قرار می‌گیرد، به‌ویژه در دوره‌های اعتراضات سیاسی مانند آنچه در ایران شاهد هستیم.

این پروتکل 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 ماهواره‌ای تأکید شده است.

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 تاثیرات 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 موثر 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 به‌شدت 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، تاثیرات 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 تاثیرات

- **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 تاثیرات:** تاثیرات قطع اینترنت بر جامعه یا سازمان خود را ارزیابی کنید. این امر شامل بررسی اختلال در ارتباطات، دسترسی به خدمات ضروری، تاثیرات 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 به‌صورت 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، دربربگیرد. 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 جمع‌آوری‌شده 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.

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.
- **واتس‌اپ:** 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 رمزگذاری‌شده 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 استفاده از 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 به‌صورت 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.
- **Inmarsat یا Iridium :** 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.

VPNها و ابزارهای ناشناس‌سازی

اگرچه VPNها P2P نیستند، اما برای دور زدن سانسور و تأمین امنیت فعالیت‌های آنلاین ضروری هستند:

- **BeePass** : یک VPN ساده و امن منبع‌باز است که برای حفظ حریم خصوصی کاربران و عبور از سانسور اینترنت طراحی شده است.
- **Tor Browser** : ترافیک اینترنت را ناشناس می‌کند و به محافظت در برابر نظارت کمک می‌کند. به‌ویژه در محیط‌هایی که فعالیت‌های مرور نیاز به محرمانگی دارد، مفید است.
- **ProtonVPN** : این سرویس VPN بسیار امن، حفاظت‌های حریم خصوصی قوی ارائه می‌دهد و با ProtonMail یکپارچه شده است.
- **Psiphon** : یک ابزار دور زدن محدودیت‌ها که ترکیبی از VPN، SSH و فناوری‌های پروکسی HTTP را ارائه می‌دهد و در کشورهایی با سانسور شدید اینترنت بسیار استفاده می‌شود.
- **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 Wiregaurd، ارتباطات را رمزگذاری می‌کند و با تنظیمات ویژه خود، به دور زدن سانسور اینترنت و حفظ حریم خصوصی کاربران کمک می‌کند. این این ابزار با ترکیب ویژگی‌های برتر Wiregaurd و دیگر فناوری‌های مرتبط، دسترسی امن و آسان را به اینترنت آزاد فراهم می‌سازد. از اینجا می‌توانید به اوپن سورس این وی‌پی‌ان 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 به‌اشتراک‌گذاری اطلاعات از طریق قرار دادن USBها در مکان‌های عمومی است که دیگران می‌توانند داده‌ها را از آن‌ها دریافت کنند. این روش که در مقایسه کمتر «تکنولوژیک» محسوب می‌شود برای توزیع اطلاعات در زمان قطع شدید اینترنت موثر است.
- **درایوهای USB رمزگذاری‌شده:** از درایوهای USB با رمزگذاری سخت‌افزاری برای ذخیره و انتقال امن اطلاعات حساس استفاده کنید. این ابزارها می‌توانند برای به اشتراک گذاشتن فایل‌های مهم به‌صورت حضوری و بدون اتکا به شبکه‌های دیجیتال استفاده شوند.
- **Ceno** : مرورگر (Cenoمخفف censorship.no!) یک مرورگر موبایل است که از روش‌های P2P برای عبور از سانسور استفاده می‌کند و به کاربران امکان می‌دهد 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، به‌طوری 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 به‌طور ایمن ارسال کنید.

مخفی‌سازی داده‌ها (Data Hiding)

مخفی‌سازی داده‌ها یا استگانوگرافی به عملیاتی گفته می‌شود که در آن اطلاعات حساس درون فایل‌های غیر مشکوک مخفی می‌شود. برخی از ابزارهای امن و مؤثر برای مخفی‌سازی داده‌ها عبارتند از:

- **Steghide :** یک ابزار محبوب استگانوگرافی یا پنهان‌سازی است که به کاربران امکان می‌دهد داده‌ها را درون فایل‌های تصویری یا صوتی پنهان کنند. این ابزار از فرمت‌های مختلفی مانند BMP, JPEG, WAV و AU پشتیبانی می‌کند. داده‌های پنهان شده با استفاده از یک گذرواژه رمزگذاری می‌شوند، که یک لایه امنیتی اضافی فراهم می‌کند.
  - از چندین فرمت فایل پشتیبانی می‌کند.
  - از رمزگذاری قوی (AES) استفاده می‌کند.
  - امکان جاسازی و استخراج داده‌ها از فایل‌ها را به‌سادگی فراهم می‌کند.
- **SilentEye :** یک اپلیکیشن استگانوگرافی یا پنهان‌سازی دیگر است که به کاربران امکان می‌دهد داده‌ها را در فایل‌های تصویری و صوتی مخفی کنند. این اپلیکیشن دارای رابط کاربری گرافیکی ساده است که استفاده از آن را آسان می‌کند. SilentEye همچنین از رمزگذاری برای حفاظت از داده‌های مخفی‌شده پشتیبانی می‌کند.
  - رابط کاربری گرافیکی کاربر پسند.
  - پشتیبانی از فایل‌های تصویری BMP، JPG و صوتی WAV
  - رمزگذاری اختیاری برای داده‌های مخفی‌شده.
- **Crypture :** یک ابزار سبک و کاربردی برای استگانوگرافی است که داده‌ها را در قالب فایل‌های تصویری BMP مخفی می‌کند. این ابزار برای افرادی که به دنبال ابزاری بدون پیچیدگی‌های اضافه هستند، مناسب است.
  - سبک و ساده برای استفاده.
  - رمزگذاری داده‌های مخفی.
  - تمرکز بر روی فایل‌های تصویری BMP.
- **Stegano :** یک کتابخانه استگانوگرافی مبتنی بر پایتون است که می‌توان از آن برای مخفی‌سازی داده‌ها در تصاویر استفاده کرد. این ابزار بیشتر برای کاربرانی مناسب است که با برنامه‌نویسی آشنایی دارند، زیرا به دانش کدنویسی برای استفاده مؤثر نیاز دارد.
  - کتابخانه پایتون برای پیاده‌سازی سفارشی استگانوگرافی.
  - قابلیت ادغام در سایر برنامه‌ها.
  - پشتیبانی از مخفی‌سازی داده‌ها در فایل‌های PNG
- **Camouflage :** یک ابزار استگانوگرافی یا پنهان‌سازی است که فایل‌ها را در فایل‌های دیگر مانند اسناد یا تصاویر مخفی می‌کند. این ابزار همچنین داده‌های مخفی‌شده را فشرده و رمزگذاری می‌کند تا تشخیص آن‌ها سخت‌تر شود.
  - مخفی‌سازی فایل‌ها درون فایل‌های دیگر مانند تصاویر و اسناد.
  - فشرده‌سازی و رمزگذاری داده‌ها.
  - رابط کاربری ساده برای استفاده آسان.

- **DeepSound:** ابزاری برای مخفی‌سازی داده‌ها در فایل‌های صوتی است. این ابزار قابلیت جاسازی فایل‌های مخفی‌شده در آهنگ‌های صوتی را بدون تغییر محسوس کیفیت صدا دارد که تشخیص آن را دشوار می‌کند.
  - تخصص در فایل‌های صوتی.
  - پشتیبانی از فرمت‌هایی مانند WAV، FLAC و سایر فرمت‌ها.
  - دارای رمزگذاری AES
- **Outguess:** یک ابزار پیشرفته استگانوگرافی یا پنهان‌سازی است که بر روی تصاویر تمرکز دارد. این ابزار طوری طراحی شده است که داده‌ها 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 مخفی‌سازی داده‌ها در تصاویر.
  - تغییرات حداقلی در تصویر حامل.
  - پشتیبانی از فرمت‌های فایل JPEG و PNM
- Tella : یک اپلیکیشن موبایل امن است که برای فعالان، روزنامه‌نگاران و مدافعان حقوق بشر طراحی شده است تا اطلاعات حساس را در محیط‌های چالش‌برانگیز مستندسازی و محافظت کند. این اپلیکیشن به طور خودکار عکس‌ها، ویدئوها و ضبط‌های صوتی را رمزگذاری کرده، آن‌ها را از گالری معمولی گوشی مخفی می‌کند و به کاربران اجازه می‌دهد برای حفاظت بیشتر از پین یا رمز عبور استفاده کنند. Tella همچنین از جمع‌آوری داده به‌صورت آفلاین پشتیبانی می‌کند و با پلتفرم‌هایی مانند Uwazi و Kobotoolbox یکپارچه می‌شود. این اپلیکیشن رایگان، چند زبانه، منبع‌باز است و برای مقابله با سرکوب فیزیکی و دیجیتالی طراحی شده است.
  - محافظت از سرکوب فیزیکی و دیجیتالی در هنگام جمع‌آوری و ذخیره اطلاعات حساس.
  - محافظت از داده‌ها در برابر سانسور، دست‌کاری، رهگیری و تخریب.
  - تولید مستندات با کیفیت بالا، که می‌توان از آن برای تحقیقات، دفاع و عدالت انتقالی استفاده کرد.
  - رمزگذاری فایل‌ها: این اپلیکیشن به محض ثبت عکس‌ها، ویدئوها و ضبط‌های صوتی، آن‌ها را به‌طور خودکار رمزگذاری می‌کند.
  - مخفی‌سازی فایل‌ها در دستگاه: فایل‌های شما از گالری و فایل اکسپلورر معمولی گوشی در دسترس نیستند و فقط در داخل اپلیکیشن قابل مشاهده‌اند.
  - قفل‌گذاری فایل‌ها: برای حفاظت از فایل‌ها یک پین یا رمز عبور تنظیم کنید. وارد کردن قفل صحیح تنها راه رمزگشایی فایل‌های ذخیره‌شده در Tella است.
  - پنهان‌سازی ظاهر اپلیکیشن: ظاهر Tella را تغییر دهید تا برای افرادی که گوشی شما را جستجو می‌کنند، مخفی بماند.
  - دوربین و ضبط‌کننده داخلی: عکس بگیرید و ویدئوها و فایل‌های صوتی را مستقیماً در Tella ضبط کنید تا فایل‌ها بلافاصله رمزگذاری و در داخل اپلیکیشن مخفی شوند.
  - Tella با Kobotoolbox، Uwazi و Tella Web یکپارچه و هماهنگ می‌شود. پلتفرمی را انتخاب کنید که به بهترین شکل با نیازهای شما همخوانی دارد و داده‌ها را مستقیماً در Tella جمع‌آوری کنید.
  - حالت آفلاین: در مناطق با اینترنت محدود یا قطع‌شده، داده‌های خود را ذخیره کنید و در زمانی که به اتصال اینترنت مطمئن دسترسی دارید، آن‌ها را ارسال کنید.

حذف فراداده‌ها

در زمان قطع اینترنت، فراداده‌ها نقش مهمی دارند و اغلب به‌اندازه 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 به‌وسیله 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 ماموران 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 جمع‌آوری‌شده 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 رمزگذاری‌شده، 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 شک‌برانگیز 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 رمزگذاری‌شده) 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، VPN ها 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 به‌اندازه 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 اشتراک‌گذاری فایل به‌صورت ناشناس)**
  - **کارکرد:** OnionShare به کاربران امکان می‌دهد فایل‌ها را به‌صورت امن و ناشناس با استفاده از شبکه Tor به اشتراک بگذارند و فراداده‌های مرتبط با فرآیند اشتراک‌گذاری را پنهان کند.
  - **نحوه استفاده:** کاربران غیر فنی می‌توانند OnionShare را نصب کرده، فایل‌های خود را به‌سادگی 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 وب‌گردی و ارتباطات)**
  - **کارکرد:** مرورگر Tor ترافیک اینترنتی کاربران را از چندین گره عبور داده و فراداده‌هایی مانند آدرس IP و عادت‌های 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 به‌طور خودکار ترافیک شما را ناشناس می‌کند.
  - **امکان استفاده:** برای ویندوز، macOS، لینوکس و اندروید.
- **Simple PDF Metadata Remover (حذف فراداده PDF)**
  - **کارکرد:** این ابزار به‌صورت 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 به‌سادگی کشیده و رها کرده و با یک کلیک فراداده‌ها را حذف کنند.
  - **در دسترس بودن:** به‌عنوان یک برنامه ساده برای ویندوز.
- **BleachBit (برای پاک‌سازی کلی فایل‌ها)**
  - **کارکرد:** BleachBit ابزاری کاربرپسند است که به حذف فراداده‌ها از انواع مختلف فایل‌ها و پاک‌سازی 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 پاک‌سازی کنند (مانند تاریخچه مرورگر، فراداده‌ها و بیشتر) انتخاب کرده و با یک کلیک پاک‌سازی 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 به‌طور خودکار فراداده‌ها را حذف می‌کند.
- **سیستم‌عامل Tails (برای حفظ کامل حریم خصوصی)**
  - **کارکرد:** Tails یک سیستم‌عامل متمرکز بر حریم خصوصی است که از طریق USB اجرا می‌شود و تمام فعالیت‌ها را ناشناس می‌کند. این سیستم‌عامل به‌صورت پیش‌فرض با ابزارهایی مانند Tor، ارتباطات رمزگذاری‌شده و حذف فراداده برای فایل‌ها بارگذاری شده است.

- **نحوه استفاده:** نصب Tails ممکن است به دانش فنی مختصری نیاز داشته باشد، اما پس از راه‌اندازی، تمام ابزارها ساده و برای حریم خصوصی از پیش تنظیم شده‌اند، که آن را برای کاربران غیر فنی که به حفاظت جامع نیاز دارند، ایده‌آل می‌کند.
- **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، روش‌های ساده و موثری برای حذف یا پنهان کردن فراداده‌ها ارائه می‌دهند و با رابط‌های کشیدن و رها کردن، پاک‌سازی با یک کلیک، و ابزارهای ناشناس‌سازی مانند Tor یا Tails پیچیدگی‌های فرآیند را به‌صورت خودکار انجام می‌دهند.