راهنمای عملی امنیت دیجیتال و ناشناسی در شبکه

آموزش جامع استفاده از شبکه Tor و سیستم‌عامل Tails

تهیه و تدوین توسط: موسسه دموکراسی و توسعه افغانستان (ADDO)

تاریخ انتشار: جون ۲۰۲۶

توهم «فضای ابری»: اینترنت واقعاً چیست؟

- اینترنت نامرئی نیست: شبکه‌ای کاملاً فیزیکی از کابل‌ها، پایه‌های مخابراتی و دستگاه‌هاست.
- گذرگاه اجباری: پیام شما قبل از خروج از کشور، حتماً از تجهیزاتِ فیزیکیِ شرکت‌هایی مثل روشن، اتصالات یا MTN عبور می‌کند.
- قانون اول امنیت: هر نهادی که این کابل‌ها و پایه‌ها را کنترل کند، می‌تواند مسیر رفت‌وآمد داده‌ها را زیر نظر بگیرد.

ردپای دیجیتال: هر کلیک، یک جای پا

- در اینترنت، هیچ‌چیز پاک نمی‌شود. هر بار که روی یک لینک کلیک می‌کنید، صفحه‌ای را باز می‌کنید یا پیامی می‌فرستید، در حالِ ثبتِ یک «جای پای نامرئی» اما ابدی هستید

- شرکت‌های مخابراتی و استخبارات با وصل کردنِ این جای پاها به همدیگر، یک «نقشه‌ی راه» دقیق از شما ترسیم می‌کنند. آن‌ها دقیقاً می‌فهمند شما از کجا حرکت را شروع کرده‌اید (مبدأ)، در مسیر به چه جاهایی سر زده‌اید، و در نهایت کجا متوقف شده‌اید (مقصد).

فعالیت‌های خاموش: چه کارهایی ردپا می‌سازند؟

- بازدید خاموش: باز کردن یک صفحه وب سایت، IP و مشخصات دستگاهِ شما را به عنوان یک بازدیدکننده در سرورهای آن‌ها ثبت می‌کند.
- میزان توقف (مکث): شبکه‌های اجتماعی الگوریتم‌هایی دارند که دقیقاً اندازه می‌گیرند شما روی یک عکس یا متن چند ثانیه مکث کرده‌اید. توقف شما، به آن‌ها می‌فهماند که به چه چیزی علاقه دارید یا از چه چیزی می‌ترسید.
- موقعیت‌یابی ناخواسته: حتی اگر GPS (مکان‌یاب) گوشی را خاموش کنید، تا زمانی که سیم‌کارتِ شما آنتن دارد یا وای‌فای روشن است، دستگاهِ شما در حالِ ارسالِ سیگنال‌های پنهان به دکل‌های اطراف است و مکان شما را به صورت ناخواسته افشا می‌کند

زنجیره شنود: چه کسانی به ردپای دیجیتال شما دسترسی دارند؟

- سرورهای متعلق به شرکت‌های ارائه‌دهنده‌ی اینترنت (مثل روشن یا اتصالات) به صورت خودکار و ۲۴ ساعته، زمانِ دقیق اتصال ، حجم دیتای مصرفی و لیستِ وب‌سایت‌هایی که بازدید کرده‌اید را در خود ذخیره می‌کنند.

- دولت‌ها و استخبارات نیازی به هک کردن موبایل شما ندارند! بلکه با فشار و حکم قانونی، کلِ این تاریخچه را از شرکت مخابرات تحویل می‌گیرند.

تصور نادرست: آیا حذف History (تاریخچه) ما را مصون می‌سازد؟

- پاک کردن تاریخچه (History)، فقط ردپای شما را از روی دستگاه خودتان (کمپیوتر یا موبایل) حذف می‌کند.

- هر سایتی که باز می‌کنید، قبل از اینکه روی مرورگر شما نمایش داده شود، از سرورِ شرکت مخابرات عبور کرده است. شما تاریخچه را از روی گوشی یا کامپیوتر خود پاک می‌کنید، اما یک نسخه‌ی کپی و غیرقابل‌حذف از تمامِ کارهای شما، برای همیشه روی سرورهای شرکتِ ارائه‌دهنده‌ی اینترنت باقی می‌ماند.

آدرس آی‌پی (IP Address) چیست؟

- در دنیای واقعی برای رساندن یک نامه، آدرس فرستنده و گیرنده باید روی پاکت نوشته شده باشد.
- در اینترنت هم دستگاه شما (کمپیوتر یا موبایل) برای دریافت معلومات به یک «آدرس دیجیتال» نیاز دارد که به آن IP می‌گویند.

آی‌پی (IP) چگونه موقعیت و هویت ما را فاش می‌کند؟

- آی‌پی مثل پیش‌شماره‌ی تلفن عمل می‌کند و بلافاصله ولایت و کشور شما را روی نقشه مشخص می‌کند.

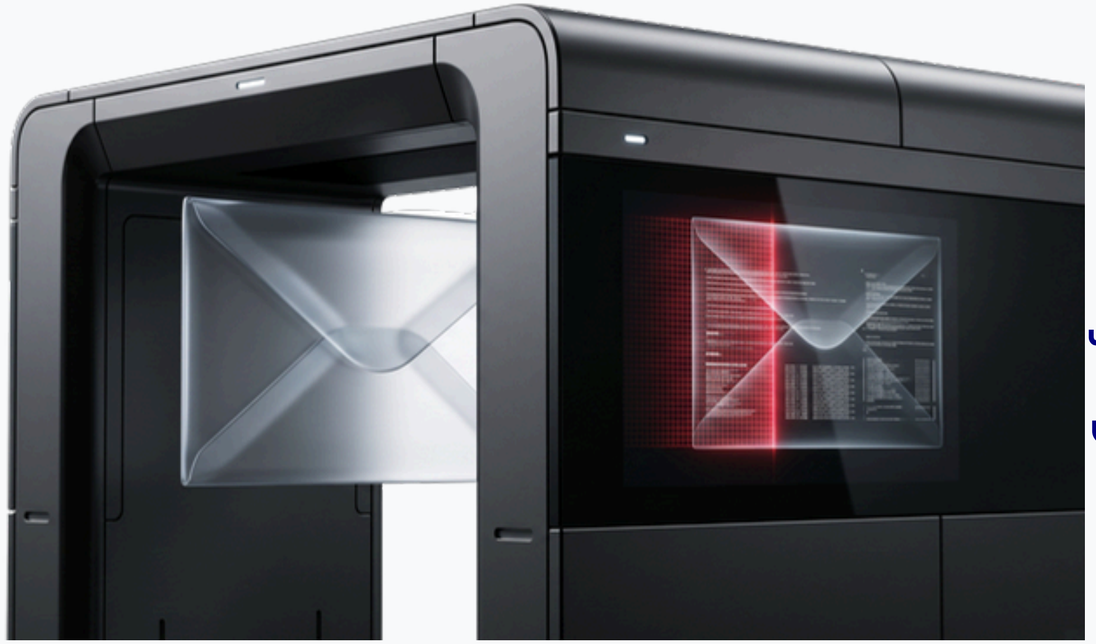
- آی‌پی همچنین افشا می‌کند که شما الان از اینترنتِ کدام شرکت (مثلاً روشن، اتصالات یا افغان بی‌سیم) استفاده می‌کنید.

- وقتی استخبارات بداند شما از کدام شرکت اینترنت گرفته‌اید، سراغ همان شرکت می‌رود و با بررسی شماره‌ی سیم‌کارت، به تذکره و هویتِ فیزیکیِ شما در دنیای واقعی می‌رسد

شرکت‌های مخابراتی (ISP) چگونه فعالیت‌های ما را نظارت می‌کنند؟

- در حالت اول پیام شما مانند یک کارت‌پستال بدون پاکت است؛ شرکت مخابراتی می‌تواند متن، عکس‌ها و مقصد پیام را کاملاً بخواند.
- در حالت دوم پیام داخل یک پاکت بسته قرار دارد؛ شرکت مخابراتی نمی‌تواند محتوای آن را بخواند، اما نام وب‌سایت (مقصد) و ساعت دقیق بازدید شما را می‌بیند.

دولت‌ها و نهادهای استخباراتی چگونه شنود می‌کنند؟



- با دستور مستقیم به شرکت‌های مخابراتی برای تسلیم‌دهی تمام گزارش‌های فعالیت و ترافیک انترنتی سیم‌کارت‌ها.

- با نصب دستگاه‌های پیشرفته در شرکت ارتباطات زیرساخت که بعد از مراکز مخابراتی و قبل از خروج از کشور جهت اسکن و تحلیلِ خودکارِ تمام ارتباطات و مقصدهای شما قرار دارد

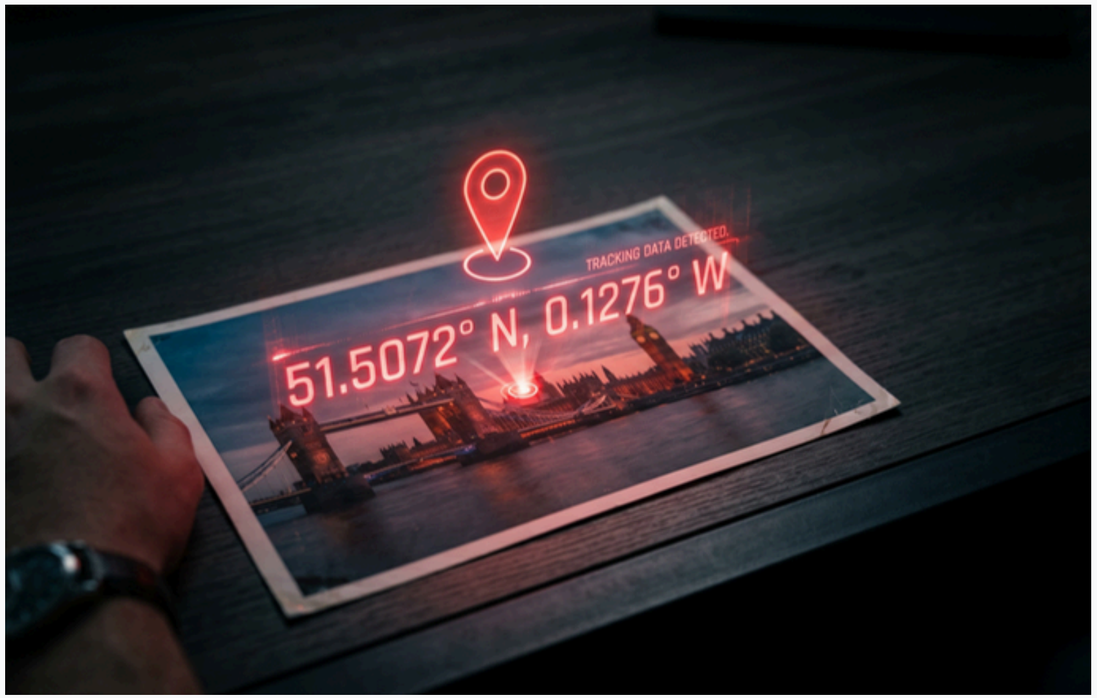
متادیتا (Metadata) یا معلومات پنهان چیست؟

- در گذشته وقتی عکسی گرفته می‌شد تاریخ و مکان آن را با قلم در پشت عکس می‌نوشتند در دنیای دیجیتال نیازی این کار نیست. وقتی شما با موبایلتان عکس می‌گیرید یا یک فایلِ وُرد (Word) می‌سازید، دستگاهِ شما صدها خط کُد را در پس‌زمینه‌ی آن فایل جاسازی می‌کند.

- متادیتا یا معلومات پنهان موقعیت دقیق جغرافیایی (GPS)، تاریخ و ثانیه‌ی ایجاد فایل، و مدلِ دستگاه شما (موبایل یا کامپیوتر) را فاش می‌کند

متادیتا = تذکره‌ی هویتیِ پنهان، که همراه با هر فایلِ شما سفر می‌کند!

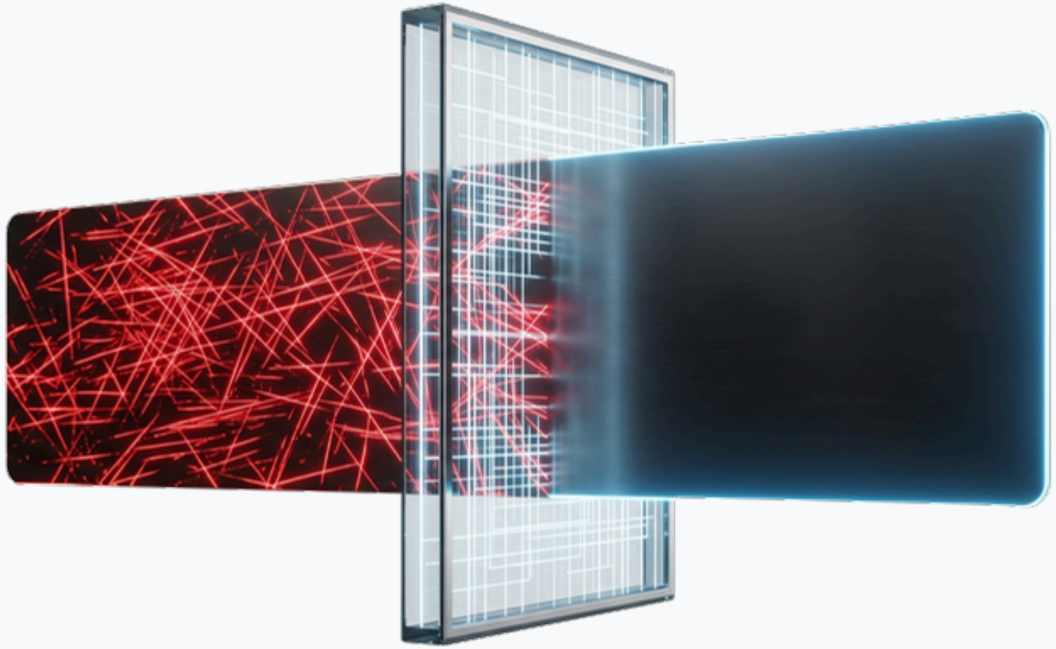
قاتل خاموش امنیت، خطر اصلی متادیتا چیست؟



- فرض کنید یک فعال مدنی با یک ایمل کاملاً ناشناس، عکسی را به خارج روان می‌کند. ابزارهای امنیتی مسیر ارتباطی او را کاملاً پنهان نگه می‌دارند.
- نهادهای استخباراتی با بررسی متادیتای خودِ عکس، ساعت دقیق، مدل موبایل و موقعیت مکانی خانه او را پیدا می‌کنند!

مسیر حرکت پنهان بود، اما خودِ فایل موقعیت شما را برملا می‌کرد!

درس بزرگ: چگونه فایلی که روان می‌کنیم، هویت ما را برملا نکند؟



- واقعیت برنامه‌ها: ابزارهای امنیتی فقط مانند یک موتر زرهی، مصونیت شما را در طول مسیر تأمین می‌کنند.
- خطر اصلی: اگر داخل این موتر زرهیِ امن، فایلی همراه با متادیتا (بمب) بگذارید، در مقصد هویت شما افشا خواهد شد.
- راه‌حل قطعی: در محیط‌های حساس، هرگز عکس، ویدیو یا هیچ فایلی را بدون پاک کردن متادیتا روان نکنید.
- ابزار پاک‌سازی (خبر خوب): سیستم‌عامل «تیلز» (Tails) ـ که به زودی با آن آشنا می‌شویم ـ یک ابزارِ قدرتمند و پیش‌فرض به نام (Metadata Cleaner) دارد. این ابزار تنها با یک کلیک، تمام این «بمب‌های پنهان» را پیش از ارسال خنثی می‌کند.

رمزنگاری (Encryption) چیست؟ (قفل‌گذاری روی پیام)

- استعاره صندوقچه: قرار دادن مکتوب محرمانه در داخل یک صندوقچه فولادی و قفل کردن آن جهت جلوگیری از خوانده شدن آن توسط پست‌رسان.
- واقعیت دیجیتال: درهم‌ریختن و قفل شدنِ پیام‌ها در شبکه‌ی انترنت؛ به طوری که هیچ‌کس در طول مسیر (حتی شرکت مخابرات) کلیدِ باز کردن و خواندنِ آن را نداشته باشد.
- نمونه‌های مصون: برنامه سیگنال (Signal) یا وب‌سایت‌های دارای قفل سبز (HTTPS).

اشتباه بزرگ: آیا قفل بودن پیام برای تأمین امنیت کافی است؟

- برنامه‌هایی مانند سیگنال: متن پیام شما را در داخل یک صندوقچه قفل می‌کنند (محتوا پنهان است).
- مشکل اصلی: قفل‌گذاری روی پیام، آدرس آی‌پی (IP) و هویت شما را پنهان نمی‌سازد!
- دیدگاه شرکت مخابراتی: شرکت مخابراتی دقیقاً می‌بیند که "شخصی با این آدرس آی‌پی در کابل، در حال ارسال یک صندوقچه قفل‌دار به خارج است."

بعضی مواقع همین که بفهمند شما با چه کسی در ارتباط هستید، برای دستگیری‌تان کافی است!

وی‌پی‌ان (VPN) چیست؟ (پست‌رسان خارجی)

- تونل مصون: دستگاه شما یک تونل قفل‌دار به سرور VPN (مثلاً در جرمنی) ایجاد می‌کند.
- شرکت مخابراتی چه می‌بیند؟ فقط می‌بیند که به جرمنی وصل شده‌اید؛ اما هرگز نمی‌داند کدام وب‌سایت را باز کرده‌اید!
- پست‌رسان خارجی (VPN) چه می‌کند؟ آدرس افغانستان شما را حذف نموده و آدرس آی‌پی خودش (جرمنی) را روی مکتوب می‌نویسد.
- وب‌سایت مقصد چه می‌بیند؟ وب‌سایت مقصد فقط یک کاربر ناشناس از کشور جرمنی را مشاهده می‌کند.

تصور نادرست از امنیت کامل: نقطه ضعف اساسی VPN کجاست؟

- جابه‌جاییِ اعتماد، نه حذفِ خطر: با روشن کردن VPN، مخابراتِ شما دیگر نمی‌داند به چه سایتی می‌روید؛ اما در عوض، خودِ شرکت سازنده‌ی VPN به عنوان واسطه‌ی جدید، تمام فعالیت‌ها، مقصدها و دیتای شما را به وضوح می‌بیند!
- تجارتِ پنهان در VPN های رایگان: آن‌ها هزینه‌های خود را از طریقِ ثبت و فروشِ تاریخچه‌ی فعالیت‌های شما (Log) به شرکت‌های تبلیغاتی یا نهادهای دولتی تأمین می‌کنند. (شما خودتان محصول هستید!)
- توهمِ امنیت در نسخه‌های پولی: حتی شرکت‌های معتبر و پولی هم ممکن است تحت فشارِ قوانین بین‌المللی یا دولت‌ها، مجبور شوند تمام گزارشِ فعالیت‌های شما را تسلیم کنند.

نتیجه‌گیری: آیا VPN برای فعالیت‌های حساس کافی است؟

- برای فعالیت‌های روزمره: VPN برای امور معمولی (مانند یوتیوب و فیسبوک) یک سپر اولیه و عالی است.
- برای فعالیت‌های حساس (امنیتی و حیاتی): هرگز نمی‌توانیم تمام معلومات محرمانه خود را به یک «شرکت واحد» در خارج از کشور بسپاریم.
- اصل عدم اعتماد: در موضوعات حیاتی، نمی‌توانیم فقط "امیدوار باشیم" که آن‌ها معلومات ما را به فروش نمی‌رسانند!

راه حل نهایی: وقتی به هیچ شرکتی نمی‌توان اعتماد کرد، چه باید کرد؟

- تغییر استراتژی: وقتی دانستیم اعتماد به یک «پست‌رسان بیرونی» (VPN) خطرناک است، باید به دنبال سیستمی باشیم که در آن اصلاً نیازی به «اعتماد کردن» به هیچ شخص یا شرکتی نباشد.
- شبکه بدون مدیریت مرکزی: ما به شبکه‌ای نیاز داریم که متعلق به هیچ شرکت، دولت یا شخص خاصی نباشد؛ سیستمی که بر اساس همکاری داوطلبانه‌ی هزاران نفر در سراسر جهان اداره شود.
- تقسیم قدرت (راز امنیت): سیستمی که در آن هیچ ایستگاهی نتواند هم‌زمان «هویت شما» و «مقصد شما» را ببیند. هر ایستگاه فقط یک بخش از معما را در اختیار دارد.
- پاسخ به این نیاز (شبکه Tor): شبکه «تور» (Tor) دقیقاً بر همین اساس ساخته شده است؛ توزیع مسیر جهت رسیدن به ناشناسی مطلق.

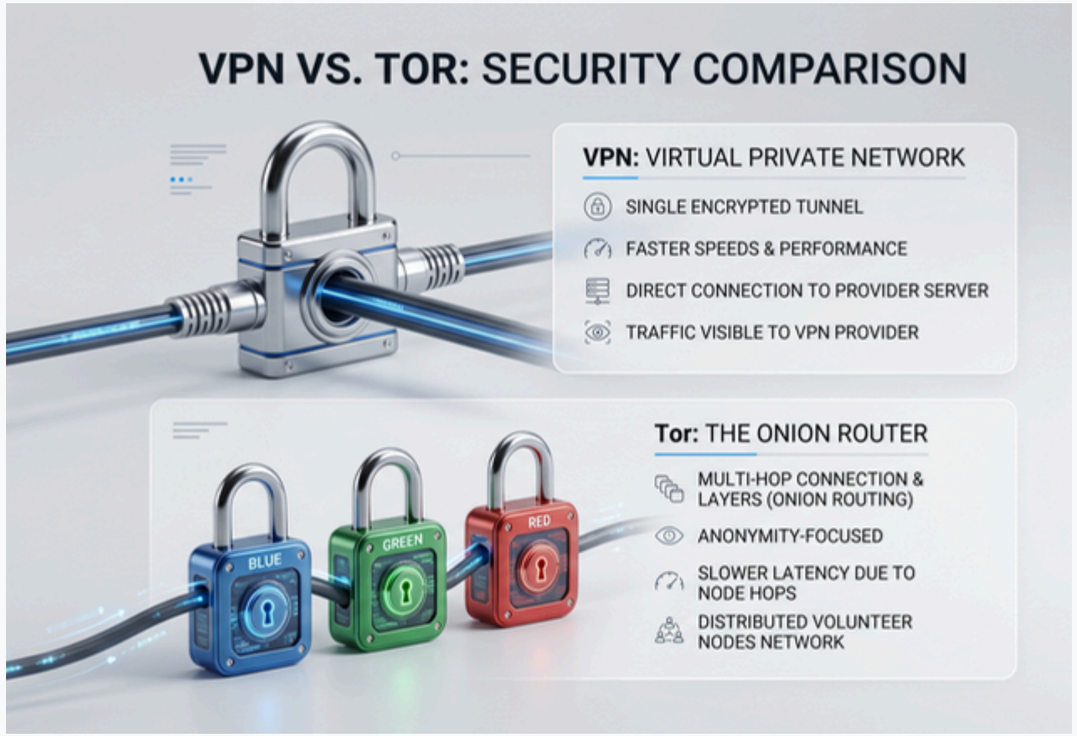
شبکه تور (Tor) چگونه کار می‌کند؟ (تمثیل پیازی)

- راز شبکه پیازی: پیام شما پیش از ارسال درون ۳ پاکت نامه‌ی تودرتو قرار می‌گیرد؛ هر ایستگاه فقط پاکت رویی را باز می‌کند تا آدرسِ ایستگاه بعدی را پیدا کند، بدون اینکَه بتواند محتوای اصلیِ پیام را بخواند.
  - ایستگاه اول (سرور نگهبان): فقط می‌داند شما چه کسی هستید، اما مقصد پیام پنهان است (پاکت اول باز می‌شود).
  - ایستگاه دوم (سرور میانی): نقطه کور! این سرور نه شما را می‌شناسد و نه از مقصد آگاه است (پاکت دوم باز می‌شود).
  - ایستگاه سوم (سرور خروجی): فقط مقصد را می‌شناسد، اما اصلاً نمی‌داند که فرستنده اصلی چه کسی است (پاکت آخر باز می‌شود).

در شبکه تور، شرکت مخابراتی مقصد شما را نمی‌بیند و وب‌سایت مقصد نیز هویت شما را نمی‌شناسد؛

شما در انترنت به یک «شبح نامرئی» تبدیل می‌شوید!

مقایسه VPN با شبکه تور (Tor): جادوی ساختار سه لایه!



- مشکل VPN (تمرکز قدرت): یک شرکت واحد، هم‌زمان هویت و مقصد شما را می‌داند. اگر این شرکت هک شود یا تحت فشارِ قانونی قرار گیرد، امنیت شما به خطر می‌افتد.
- راه حل شبکه تور (توزیع مسیر): پیام شما درون ۳ پاکت تودرتو پیچیده شده و از ۳ ایستگاه مستقل عبور می‌کند؛ به گونه‌ای که هیچ ایستگاهی هم‌زمان نمی‌داند فرستنده اصلی کیست و مقصد نهایی کجاست.

در VPN شما به «یک شرکت» اعتماد می‌کنید، اما

در Tor به «طراحیِ یک سیستمِ غیرمتمرکز و غیرقابلِ ردیابی» تکیه می‌کنید!

پل (Bridge) چیست و چگونه سانسور شدید انترنت را دور می‌زند؟

- مشکل اصلی (سدِ سانسور): آدرسِ سرورهای ورودیِ شبکه تور کاملاً عمومی است. به همین دلیل، سیستم‌های سانسورِ دولت‌ها این دروازه‌ها را به راحتی شناسایی و مسدود می‌کنند.
- راه حل (دروازه‌های مخفی): «پل‌ها» همان ایستگاه‌های ورودیِ پنهانی هستند که آدرسِ آن‌ها مخفی نگه داشته می‌شود تا سیستم‌های سانسور اصلاً از وجودشان باخبر نشوند.
- جادوی پل‌ها (تغییر قیافه ترافیک): پل‌ها بر روی پیام شما «لباس مبدل» می‌پوشانند. شرکت مخابراتی ترافیک انترنتی شما را نظارت می‌کند، اما تصور می‌کند که یک جستجوی معمولی تماس ویدیویی است!

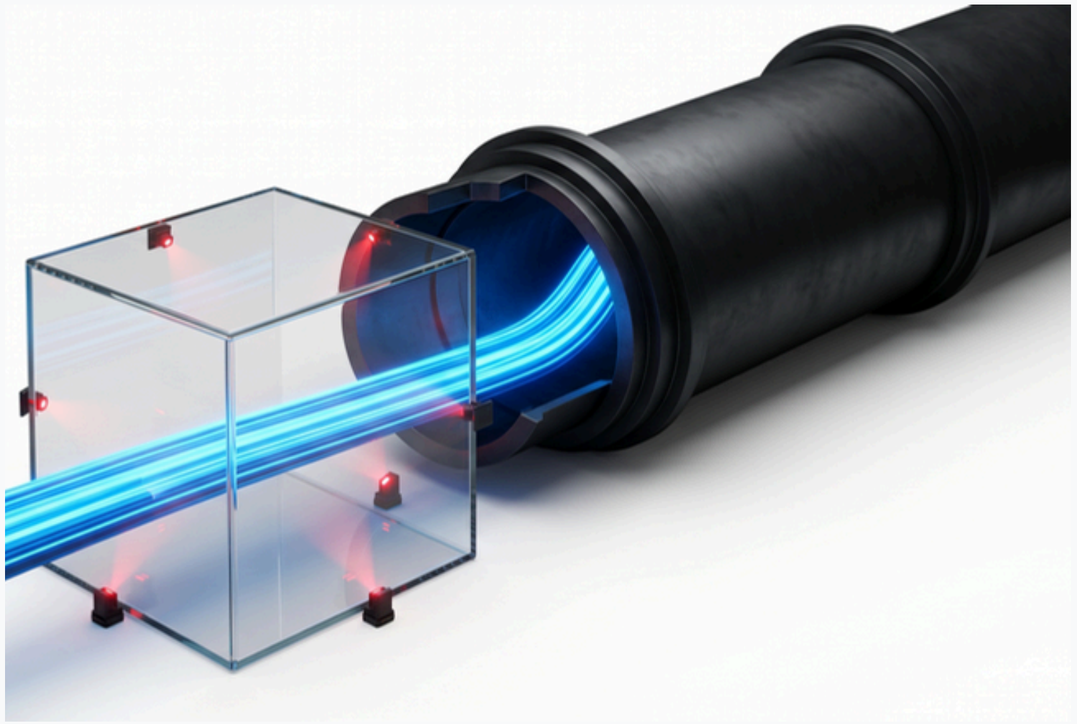
پُل (Bridge) به شما یک درِ ورودیِ مخفی و یک لباس مبدل می‌دهد تا حتی از پیشرفته‌ترین ایستِ‌بازرسی‌های انترنتی هم عبور کنید!

محدودیت‌های تور (Tor): ۴ قانونی که هرگز نباید نقض کنید!

- قانون اول؛ فدا کردنِ سرعت برای امنیت: عبور ترافیک از ۳ کشور مختلف، سرعت اینترنت را کاهش می‌دهد. تور هرگز برای دانلودهای سنگین یا تماشای آنلاینِ ویدیو ساخته نشده است.
- قانون دوم؛ تور همه‌چیز را رمزنگاری نمی‌کند: تور فقط «مسیر» را مخفی می‌کند. اگر سایتِ مقصد قفل سبز (HTTPS) نداشته باشد، ایستگاه آخر (سرور خروجی) می‌تواند تمام چت‌ها و رمزهای عبور شما را تماشا کند!
- قانون سوم؛ ممنوعیت ورود به حساب‌های شخصی: اگر با شبکه تور وارد فیس‌بوک، ایمیل یا حساب‌های کاربریِ واقعی خود شوید، تمام زحمات تور را هدر داده‌اید؛ چون سیستم‌ها بلافاصله نام و هویتِ واقعی شما را شناسایی می‌کنند.
- قانون چهارم؛ به تنظیماتِ مرورگر دست نزنید: نصب افزونه‌های اضافی یا حتی بزرگ کردنِ پنجره‌ی مرورگر (Maximize)، یک «اثر انگشتِ منحصربه‌فرد» از سیستم شما می‌سازد و ردیابیِ شما را برای سیستم‌های هوشمند ممکن می‌کند.

شبکه تور یک دیوار نفوذناپذیر است؛ اما به شرطی که خودتان با خطاهای کوچک، درِ این قلعه را روی جاسوسان باز نکنید!

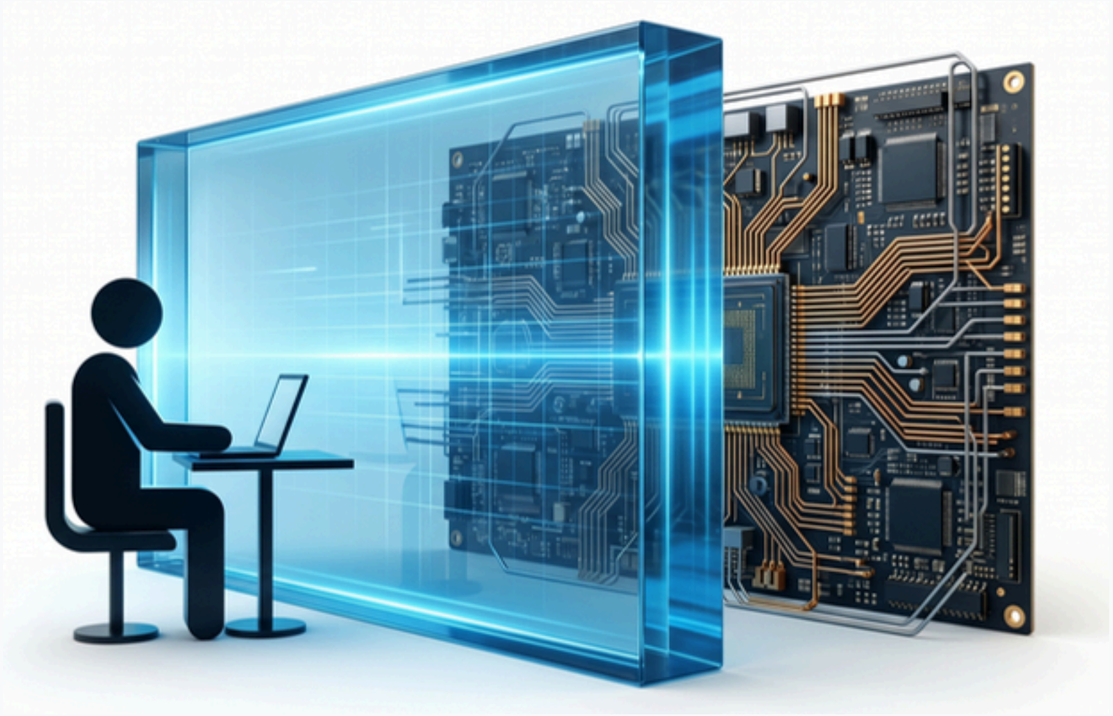
حلقه گمشده امنیت: چرا شبکه تور (Tor) به تنهایی کافی نیست؟



- واقعیت تلخ: تور (Tor) فقط مانند یک تونل زرهی است که «مسیر» پیام‌های شما را در انترنت مصون می‌سازد؛ اما روی دستگاه شما هیچ کنترلی ندارد.
- تمثیل خانه ناامن: استفاده از تور در یک کمپیوتر ناامن، مانند این است که برای سفر از یک موتر کاملاً ضد مرمی استفاده کنید، اما دروازه خانه و اتاق کار خود را برای دزدها و جاسوسان باز گذاشته باشید!
- خیانت پنهان برنامه‌ها: حتی اگر مرورگر تور باز باشد، سایر برنامه‌های کمپیوتر شما می‌توانند پنهانی و بدون عبور از تور به انترنت وصل شده و موقعیت (IP) اصلی شما را فاش سازند!
- خطر در مبدأ (داخل کمپیوتر): اگر کمپیوتر شما حاوی بدافزار باشد یا تاریخچه فعالیت‌ها روی هارد دیسک ذخیره شود، قوی‌ترین شبکه‌ها نیز هویت شما را پنهان نخواهند کرد.
- نیاز به یک محیط پاک: برای امنیت واقعی، ما به سیستم‌عاملی نیاز داریم که تمام ارتباطات خارج از تور را «مسدود» کند و هیچ ردی روی هارد دیسک باقی نگذارد.

تور (Tor) امنیت شما را در فضای «انترنت» تأمین می‌کند، اما برای مسدود کردن خیانت برنامه‌ها در داخل «کمپیوتر»، ما باید به سراغ ریشه اصلی یعنی سیستم‌عامل (OS) برویم.

پیش‌نیازِ امنیت: سیستم‌عامل (OS) دقیقاً چیست؟



- استعاره ساختمان: کمپیوتر مانند یک ساختمان بزرگ است؛ نیاز به یک «مدیر» دارد تا برق، آب و اتاق‌ها (برنامه‌ها) چگونه باید کار کنند.
- تعریف اصلی: سیستم‌عامل همان «برنامه اصلی» یا مدیر عمومی این ساختمان است.
- مثال‌های آشنا: ویندوز (Windows) در کمپیوتر، و اندروید (Android) در موبایل، همگی سیستم‌عامل هستند.

نتیجه‌گیری: بدون سیستم‌عامل، کمپیوتر و موبایل شما فقط یک تکه آهن و پلاستیک بی‌مصرف است!

چرا ویندوز ناامن است؟ (تمثیل خانه شیشه‌ای)

- جاسوسی قانونی (Telemetry): مایکروسافت به صورت پیش‌فرض، لیست برنامه‌هایی که اجرا می‌کنید و وب‌سایت‌هایی که می‌بینید را جمع‌آوری کرده و به سرورهای خود می‌فرستد.
- کتابچه‌ی جاسوسی (ردپاها): ویندوز همیشه سابقه‌ی کارهای شما را نگه می‌دارد. حتی اگر یک فایل را کاملاً حذف کنید، نامِ آن فایل در لیستِ فایل‌های اخیر (Recent Files) ویندوز همچنان باقی می‌ماند.
- حافظه‌ی تاریخی (USB): ویندوز شناسنامه‌ی دقیقِ هر فلش‌مموری که حتی یک بار به آن وصل شود را ثبت می‌کند. «اثرِ حضورِ» آن فلش برای همیشه در سیستم باقی می‌ماند.
- کدهای پنهان (جعبه سیاه): چون کدهای برنامه‌نویسی ویندوز بسته و مخفی است، هیچ‌کس در دنیا نمی‌داند آیا یک «درِ پشتی» (Backdoor) برای دسترسی سازمان‌های استخباراتی در آن باز گذاشته شده است یا خیر.
- تمرکز اصلی هکرها بر روی سیستم‌عامل ویندوز: از آنجا که بیشتر کامپیوترهای جهان (و ادارات افغانستان) از ویندوز استفاده می‌کنند، بخش اعظم بدافزارها، باج‌افزارها و ابزارهای جاسوسی دنیا دقیقاً برای هک کردن و نفوذ به ویندوز ساخته می‌شوند.

تصور نادرست از حذف فایل‌ها: فریب بزرگ دکمه Delete!

- فریب زباله‌دانی: خالی کردن Recycle Bin در ویندوز، اصلاً محتوای فایل را از روی هارد دیسک حذف نمی‌کند!
- تمثیل کتاب: ویندوز فقط نام فایل را از «فهرستِ» هارد دیسک خط می‌زند؛ اما صفحاتِ فایل هنوز دست‌نخورده باقی مانده‌اند!
- خطر بازیابی (Recovery): نیازی به تجهیزاتِ فوق‌پیشرفته‌ی استخباراتی نیست! هر کسی می‌تواند با یک برنامه‌ی ساده‌ی ریکاوری، تمام فایل‌هایی را که سال‌ها پیش حذف کرده‌اید، دوباره برگرداند.

راه حل نهایی: ما به سیستم‌عاملی نیاز داریم که مثل یک «شبح» باشد؛ سیستمی که اصلاً کاری با هارد دیسک نداشته باشد و پس از خاموش شدن، هیچ ردپایی از خود به جا نگذارد!

سیستم‌عامل «فراموش‌کار»: چرا تیلز (Tails) هیچ ردی نمی‌گذارد؟

- تفاوت هارد با رَم (RAM): هارد دیسک مانند یک «کتابچه» دائمی است؛ اما رَم (RAM) مانند یک «تخته سفید» است که به محضِ قطع شدنِ برق، در یک ثانیه کاملاً پاک می‌شود
- جادوی تیلز: این سیستم‌عامل روی یک فلش (USB) نصب می‌شود و برنامه‌هایش را مستقیماً روی تخته سفید (RAM) باز می‌کند (اصلاً به هارد شما وصل نمی‌شود!).
- تولد دوباره: تیلز هر بار که روشن می‌شود، دقیقاً مانند یک نوزاد است که هیچ پیشینه‌ای از گذشته ندارد.
- راه‌حل در لحظه‌ی خطر: فقط کافیست فلش را از کامپیوتر بیرون بکشید! با قطع شدنِ برق سیستم، تمامِ نوشته‌های روی این تخته سفید در کسری از ثانیه پاک و نابود می‌شود.

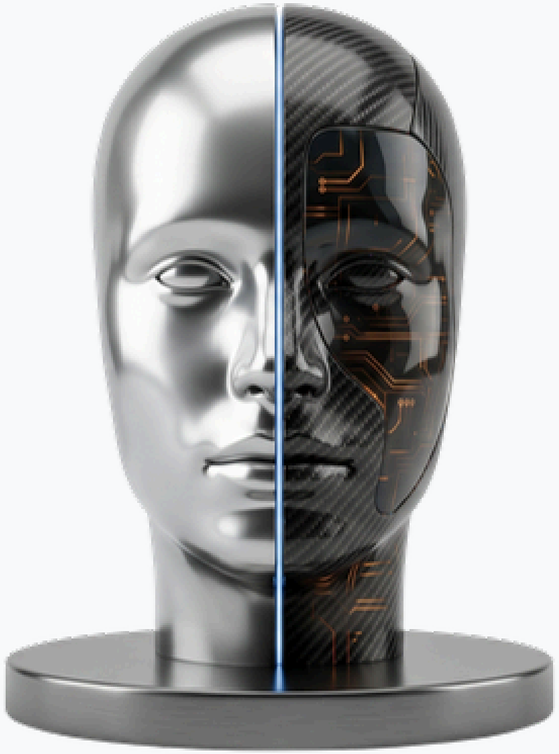
قطع برق در تیلز = نابودی کامل تمام ردپاها و تبدیل شدن به یک شبح دیجیتال!

دانلود مصون و تأیید اصالت (Verification)

- حجم فایل نصب: فایل اصلی نصب تیلز (با فورمت img.) حدود ۱/۸ گیگابایت است.
- خطر وب‌سایت‌های جعلی: هکرهای دولتی ممکن است وب‌سایتی دقیقاً شبیه وب‌سایت تیلز بسازند تا نسخهٔ دست‌کاری‌شده و خطرناک خود را به شما ارائه کنند.
- دانلودِ مخفیانه (سپرِ مخابراتی): برای جلوگیری از ردیابی و حساس شدنِ شرکت مخابرات، حتماً با VPN روشن یا از طریق مرورگر تور (Tor) این سیستم‌عامل را دانلود کنید.
- ابزارِ تأیید اصالت: وب‌سایت رسمی تیلز مکانیزمی دارد که بلافاصله پس از اتمام دانلود، فایلِ دریافت شده را اسکن و بررسی می‌کند.
- تیک سبز نجات‌بخش: این ابزار با نمایش یک «تیک سبز»، رسماً تأیید می‌کند که این فایل دقیقاً همان نسخه اصلی است و در مسیر دانلود هیچ‌گونه دست‌کاری در آن صورت نگرفته است.

حتی اگر فایل را از سایت رسمی دانلود کرده‌اید، هرگز بدون دیدنِ «تیک سبزِ اصالت»، آن را روی فلشِ خود نصب نکنید!

قانون «دو زندگی مجزا» (جداسازی هویت‌ها)



- زندگی معمولی (آشکار): با نام واقعی و حساب‌های شخصی. (این زندگی منحصراً روی ویندوز یا موبایلِ عادیِ شما جریان دارد).
- زندگی پنهان (شبح): با نام مستعار و ایمیلِ ناشناس. (این زندگی فقط و فقط باید داخل سیستم‌عامل تیلز اتفاق بیفتد).

خطر مرگبار (نشت هویت): اگر در محیط تیلز، وارد فیس‌بوک یا جیمیلِ شخصیِ خود شوید، در همان ثانیه هویتِ پنهانِ شما فاش می‌شود و سیستم‌های ردیابی می‌فهمند آن «شبح»، در واقع همان «شما» هستید!

دیوار فولادی: هرگز حساب‌های زندگیِ معمولی را داخل تیلز باز نکنید، و هرگز حساب‌های پنهانِ خود را در ویندوز بررسی نکنید.

سیستم‌عامل تیلز از شما حفاظت می‌کند، اما نمی‌تواند جلوی اشتباهات انسانی شما را بگیرد!

امنیت فیزیکی: حفاظت از تیلز در دنیای واقعی

- تهیه امن (تأمین از منبع اصلی): هرگز فلشِ آماده‌ی تیلز را از بازار یا افرادِ دیگر نخرید (خطر دست‌کاری)؛ این سیستم‌عامل را باید شخصاً و فقط از وب‌سایت رسمی (tails.net) دانلود کنید.
- خطرِ سخت‌افزارهای جاسوسی: فلشِ تیلز را هرگز به کامپیوترهای عمومی (مثل اینترنت‌کلاب‌ها) وصل نکنید. سیستم‌عامل تیلز نمی‌تواند شما را در برابرِ قطعاتِ فیزیکیِ شنود (Hardware Keylogger) که به کیبوردِ آن کامپیوتر وصل شده‌اند، محافظت کند!
- جداسازی اضطراری (Kill Switch): در لحظه‌ی احساسِ خطر، فقط کافیست فلش را از دستگاه بیرون بکشید! تیلز فوراً صفحه را تاریک، کامپیوتر را خاموش و تمامِ ردپاهای روی حافظه را کاملاً پاک و نابود می‌کند.

خطای انسانی: وقتی خودمان سپرها را می‌شکنیم!

- تمثیل موتر زرهی: تیلز یک موتر کاملاً ضد مرمی است؛ اما یک «کلیک اشتباه»، دقیقاً مانند این است که با دست خود شیشه را پایین بکشید!
- تله‌ی معلومات پنهان (Metadata): فایل‌های شما (از عکس‌ها گرفته تا اسناد Word و PDF) حاویِ اطلاعاتِ مخفی مانند نام سازنده، مدل دستگاه و موقعیت مکانی هستند. روان کردنِ این فایل‌ها بدون استفاده از ابزارِ «پاک‌سازیِ متادیتا» در تیلز، هویتِ پنهانِ شما را کاملاً فاش می‌کند!
- قانون عدم اعتمادِ مطلق (Zero Trust): در فضای امنیتی، همیشه فرض کنید تمام لینک‌ها و فایل‌های دانلودی، یک «ماینِ پنهان» هستند که دقیقاً برای نابودیِ سیستمِ شما کار گذاشته شده‌اند!

قانون طلایی کلیک: پیش از باز کردن هر لینک یا فایل، حتماً ۳ ثانیه مکث کنید!

بخش دوم: کارگاه عملی (ساخت زره دیجیتال شما)

- پایانِ تئوری: تا اینجا با منطقِ سیستم‌های جاسوسی، قوانینِ امنیت و خطراتِ پنهان در دنیای دیجیتال به خوبی آشنا شدیم.
- آغازِ عمل: اکنون واردِ فازِ عملی می‌شویم تا این «زرهِ دیجیتال» و سیستم‌عاملِ پنهانِ خود (تیلز) را گام‌به‌گام با هم خلق کنیم.
- تجهیزاتِ مورد نیاز: لطفاً تمامِ تمرکزِ خود را جمع کنید. اگر فلش‌مموریِ (USB) خود را تهیه کرده‌اید، آن را روی میز بگذارید تا کار را شروع کنیم!

آماده‌سازی فلش و نصب تیلز (Flashing)

- نیاز اولیه: یک یواس‌بی (USB) فلش با حداقل ۸ گیگابایت حافظه (توصیه: ۱۶ یا ۳۲ گیگابایت).
- برنامه واسطه: فایل تیلز را نمی‌توان به صورت معمولی (مانند عکس) کاپی کرد؛ فلش باید توسط یک برنامه به «دستگاه قابل بوت» تبدیل شود.
- ابزار پیشنهادی (Rufus): یک برنامه رایگان، مصون و بسیار ساده:
- قانون دانلود و نصب: این برنامه را فقط و فقط از وب‌سایت رسمی آن (rufus.ie) دانلود کرده و روی کمپیوتر خود باز (اجرا) کنید. دانلود از سایت‌های ناشناس برای دریافت این برنامه، یک خطر امنیتی بزرگ است.
  - فلش خود را انتخاب کنید.
  - فایل تیلز (دانلود شده) را انتخاب کنید.
  - دکمه Start را فشار داده و منتظر پایان کار بمانید.

هشدار: با فشار دادن دکمه Start، تمام معلومات و فایل‌های قبلی روی این فلش برای همیشه حذف خواهند شد!

ورود به دنیای پنهان: چگونه با فلشِ تیلز روشن شویم؟

- آمادگی: فلش زرهی شما آماده است (دقت کنید که در محیط ویندوز، فایل‌های آن نمایش داده نمی‌شود).
- قطع ارتباط با هارد: کمپیوتر را کاملاً خاموش کنید. فلش را وصل نموده و کمپیوتر را روشن کنید.
- ورود به هسته سیستم (BIOS): به محض فشار دادن دکمه روشن/خاموش، کلید بایوس (معمولاً F2، F10 یا Delete) را پی‌درپی فشار دهید تا وارد صفحه تنظیمات شوید.
- باز کردن قفل‌های ویندوز: در منوهای بایوس جستجو کنید و حتماً دو گزینه Secure Boot و Fast Boot را پیدا نموده و روی حالت Disable (غیرفعال) تنظیم کنید.
- انتخاب فلش و خروج: در همان محیط، فلش خود را در اولویت اول بوت (Boot Priority) قرار دهید. در فرجام کلید ذخیره (معمولاً F10) را فشار داده و خارج شوید.

صفحه خوش‌آمدگویی و تنظیمات حیاتیِ اتصال به تور

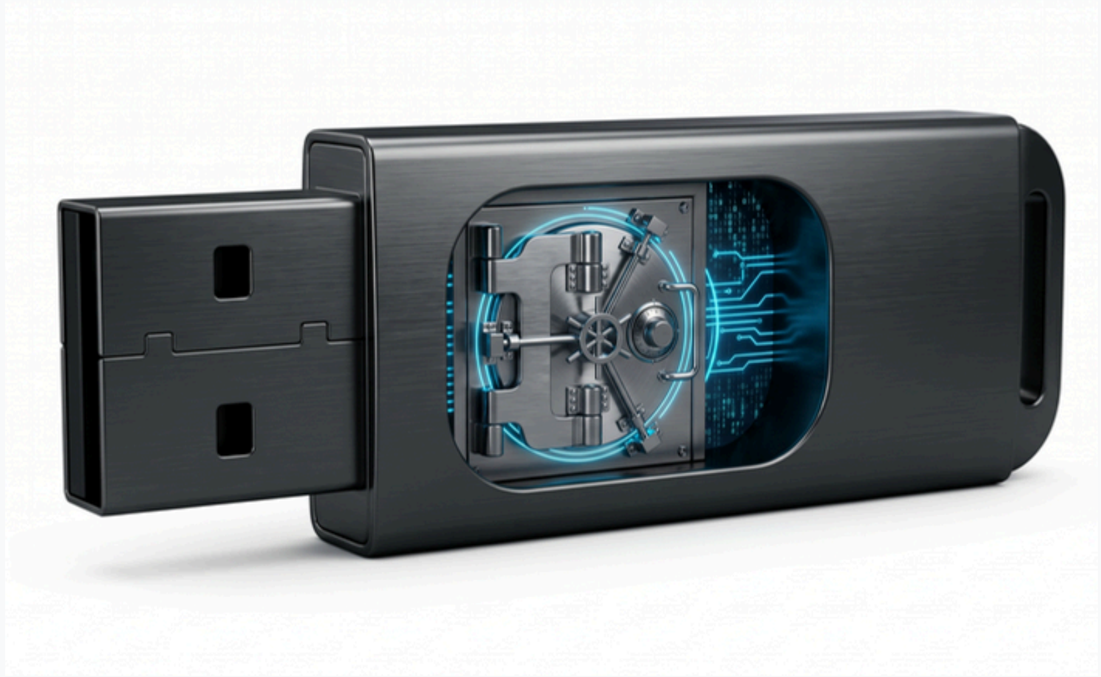
- ورود اولیه: زبان را انتخاب کنید، Start Tails را فشار دهید و به وای‌فای (Wi-Fi) وصل شوید.
- صفحه اتصال به تور (مرحله سرنوشت‌ساز): سیستم از شما می‌پرسد چگونه به انترنت وصل شود؟
  - حالت معمولی (کشورهای آزاد): اتصال مستقیم (Connect to Tor automatically).
  - حالت امنیتی (عبور از سانسور شدید): حتماً گزینه دوم یعنی پنهان‌کاری (Hide to my local network that I'm connecting to Tor) را انتخاب کنید.

قانون حیاتی برای افغانستان: همیشه از «حالت امنیتی» استفاده کنید تا شرکت مخابراتی نتواند ترافیک تور شما را شناسایی یا مسدود کند!

دریافت و وارد کردن پل (Bridges): دروازه‌های پنهان

- نیاز به پل: با انتخاب گزینه «پنهان‌کاری»، تیلز از شما آدرس یک پل (دروازه پنهان) را درخواست می‌کند.
- از کجا پل مصون دریافت کنیم؟
  - ایمیل: از یک ایمیل ناشناس، پیامی با موضوع get transport obfs4 به آدرس bridges@torproject.org روان کنید (متن ایمیل خالی باشد).
- وارد کردن پل: کدهای دریافتی را در چوکات مخصوص در تیلز کاپی نموده و دکمه Connect را فشار دهید.

گاوصندوق پنهان (Persistent Storage)



- سیستم عامل فراموش‌کار: با هر بار خاموش شدن، تیلز تمام معلومات، فایل‌ها و تنظیمات شما را کاملاً حذف می‌کند.
- ساخت گاوصندوق ضد مرمی: شما می‌توانید بخشی از فضای خالی فلش خود را به یک «گاوصندوق رمزگذاری‌شده» تبدیل کنید تا معلومات حیاتی شما از حذف شدن مصون بماند.
- دارایی‌های حیاتی: چه چیزی را در اینجا ذخیره کنیم؟ کدهای پل (Bridges)، صندوقچه‌ی رمزهای عبور (KeePass)، کیف‌پول ارز دیجیتال، قفل‌های مخفی برای پیام‌ها (PGP)، سایت‌های ذخیره‌شده‌ی تور، رمزهای وای‌فای و اسناد محرمانه.

هشدار حیاتی: اگر رمز این گاوصندوق (Passphrase) را فراموش کنید، نه‌تنها هیچ هکر و نهاد استخباراتی، بلکه «خود شما» نیز دیگر هرگز به آن دسترسی نخواهید داشت و معلومات شما برای همیشه قفل و غیرقابل بازیابی خواهد ماند.

از همراهی شما سپاسگزاریم

برای امنیت بیشتر، در فضای دیجیتال آگاهانه قدم بردارید

addo.ngo

info@addo.ngo

@ADDO_AFG

ADDO Afghanistan

ADDO Afghanistan

@AzadyDigitalCivilSociety