ایمنی در فعالیت آن‌لاین

موضوع درس‌نامه : یادگیری حفاظت از فعالیت‌های آنلاین

- **درباره‌ی اهمیت مرورگر و** https
- درباره‌ی وی پی ان VPN و تور Tor

شما حتما واژه‌ی https دیده یا شنیده‌اید. آیا می‌دانید معنای آن چیست؟

آیا می‌دانید اضافه کردن حرف S در پایان این پروتکل اینترنتی به چه معناست؟

- **آیا به نام سازنده آن یعنی شرکت** Safran است؟
- آیا حرف جمع در زبان انگلیسی است؟
- آیا به معنای **Secure یا امنیت است**؟

(HTTPS) پروتکل امن انتقال ابرمتن است و ترکیبی از پروتکل HTTP و SSL است. هدف آن فراهم آوردن ارتباطات ایمن رمزنگاری شده و شناسایی امن یک وب‌سایت است.

جهت اطلاع و آگاهی شما :

] **پروتکل** انتقال ابرمتن به اختصار اچ‌تی‌پی (http) یک پروتکل یا قرارداد ارتباطی است که برای انتقال و **تبادل** اطلاعات در وب استفاده می‌شود.

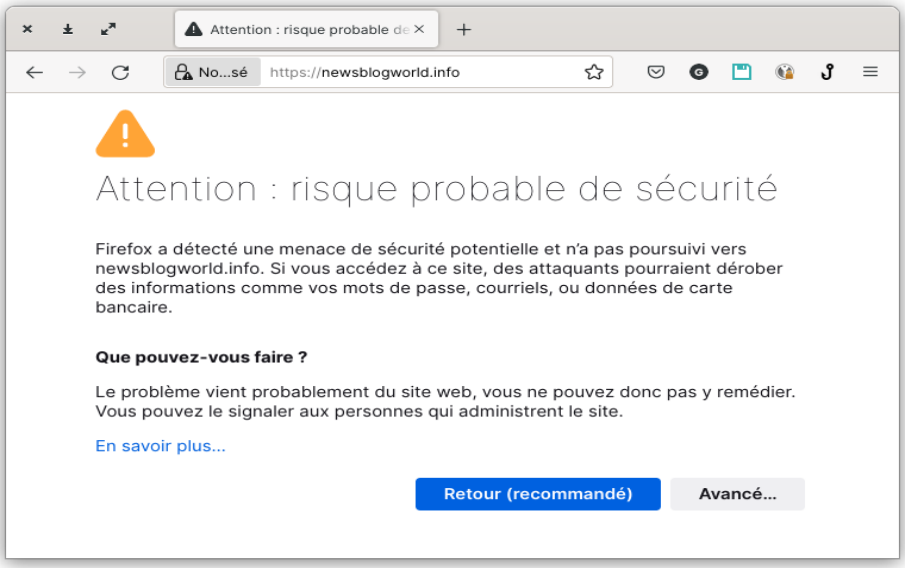
SSL مخفف Secure Socket Layer به معنی «لایه اتصال امن» و پروتکلی (مجموعه‌ای از قوانین) جهت برقراري ارتباطات ایمن میان سرویس دهنده و سرویس گیرنده در اینترنت است. [

زمانی که با آدرس اینترنتی (URL) یک وب‌سایتی با **https** آغاز می‌شود، می‌توان از سه نکته مهم اطمینان حاصل کرد:

- **اعتبارو واقعی بودن وب‌سایت** : هر وب‌سایت با پروتکل https دارای یک گواهی ایمنی (certificat) است، به هنگام بازدید از آن مرورگر شما به آن دسترسی خواهد یافت. مرورگر شما دارای یک پایگاه داده‌ها است که امکان بررسی اعتبار این گواهی را دارد. این گواهی معادل کارت شناسایی وب‌سایت است و هر وب‌سایت به صورت یگانه گواهی https خود را دارد.

- **محرمانگی اطلاعات یا داده‌ها**: میان مرورگر شما و وب‌سایت بازدید شونده، اتصال‌های گوناگونی وجود دارد؛ از ارائه‌دهنده خدمات اینترنت، سرور یا سرورها، احتمال وجود پروکسی‌های ، حتی تا فردی بد نیت (به ویژه به هنگام اتصال به وای‌فای‌های عمومی). اما پس از تأیید اعتبار وب‌سایت، یک کانال ارتباطی رمزنگاری شده میان مرورگر شما و وب‌سایت ایجاد می‌شود، تا اطمینان حاصل شود که هیچ اتصال ثالثی میان مرورگر شما و وب‌سایت بازدید شونده، نمی تواند به اطلاعات منتقل شما اعم ازصفحه‌های درخواست شده، محتوای آن‌ها یا رمزهای عبور ارسالی، دسترسی یابد.
- **صحت اطلاعات یا داده‌ها** : استفاده از پروتکل https همچنین تضمین می‌کند که هیچ‌کس نمی‌تواند اطلاعات فرستاده شده را تغییر دهد.

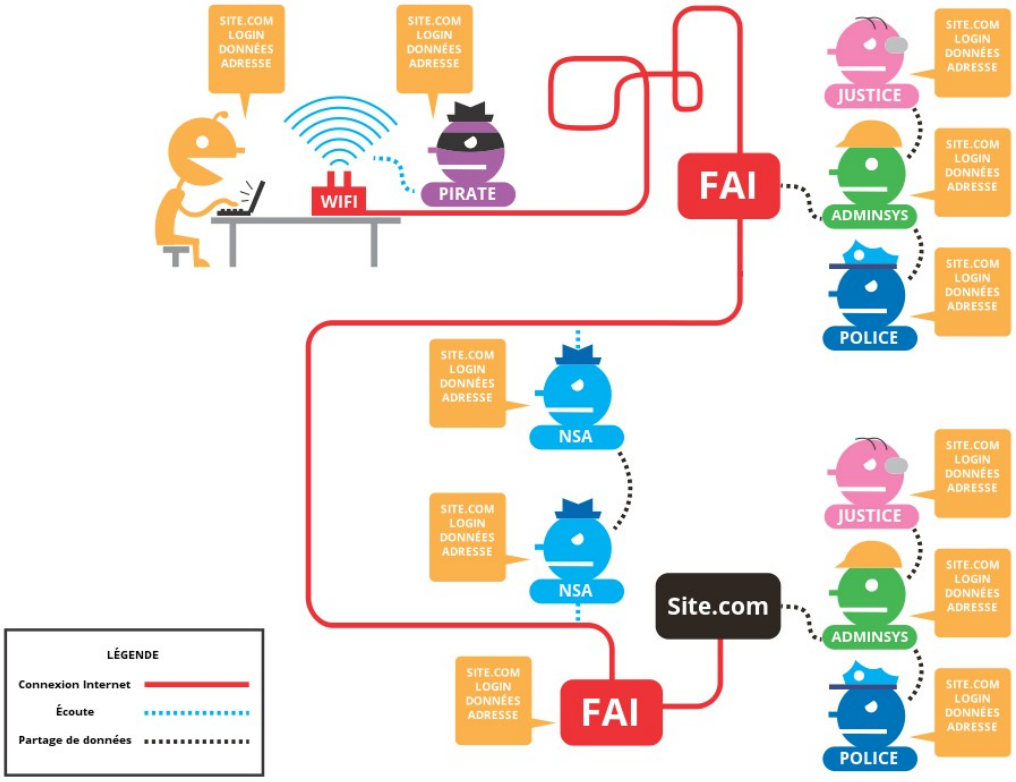
هشدارهای خطر https



هشدار HTTPS

مشاهده‌ی این هشدار به هنگام بازدید از یک وب سایت، به این معناست که مرورگر شما قادر به اطمینان یافتن از هویت واقعی وب‌سایت نیست. این هشدار نشان می‌دهد که گواهی HTTPS وب‌سایت معتبر نیست، و مرورگر به شما هشدار امنیتی می‌دهد. در یک کلام این هشدار می‌گوید: "من هویت این وب‌سایت را نمی‌توانم تایید کنم، ممکن است یک صفحه جعلی و خطرناک باشد."

با این حال، شما می‌توانید با دانستن خطر اتصال غیر ایمن به آن دسترسی پیدا کنید. چون هویت وب‌سایت مشخص نیست، ارتباط بین کامپیوتر یا گوشی هوشمند شما و وب‌سایت امن نخواهد بود، **و تمام اطلاعاتی که از اینترنت میان دستگاه شما و وب‌سایت عبور می‌کنند، رمزنگاری شده نیستند.**



استفاده درست مرورگر خود از HTTPS را تضمین کنید:

• از مرورگرهای Firefox، IE Edge یا Chrome استفاده کنید.

• افزونه Duck Duck Go Privacy Essentials را بر روی Firefox یا Chrome نصب کنید.

• برای استفاده در Android یا iOS، از مرورگر Duck Duck Privacy Browser استفاده کنید.

تمرین:

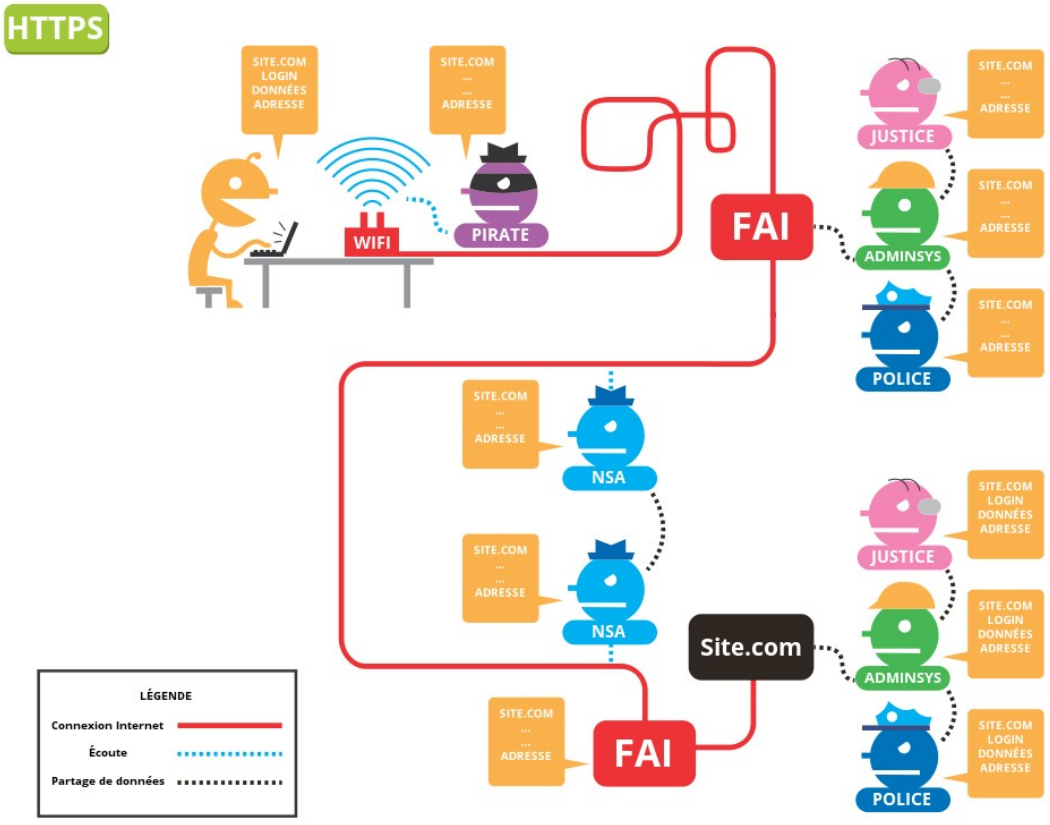
۱. افزونه Duck Duck Go Privacy Essentials را بر روی Firefox یا Chrome نصب کنید.

۲. پس از نصب افزونه، روی دکمه " 🔒 " کلیک کنید تا ببینید آیا اتصال امن است و چه وب‌سایت‌های ثالثی مسدود شده‌اند.

برای نصب افزونه اینجا را ببینید

* استفاده از HTTPS تنها وابسته به دقت و کارایی شما نیست بلکه به وب‌سایتی وابستگی دارد که در حال بازدید از آن هستید، هرچند بسیاری (نزدیک به ۸۰ %) از وب‌سایت‌ها نسخه ایمنی ارائه می‌دهند، اما این موضوع برای همه‌ی مرورگرها صادق نیست.

* HTTPS تبادل داده‌ها بین شما و وب‌سایتی که در حال بازدید از آن هستید را ایمن می‌کند، اما امانت‌دار بودن مرورگر شما در اینترنت را تضمین نمی‌کند. نام‌های دامنه وب‌سایت‌هایی که بازدید می‌کنید همچنان توسط ارائه‌دهنده خدمات اینترنت (FAI)، کارفرما یا کافه اینترنت مورد استفاده شما قابل مشاهده هستند.

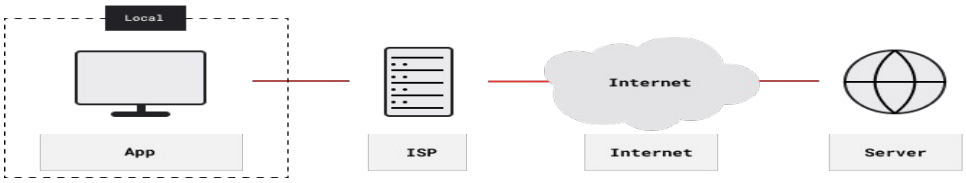


با VPN اتصال خود را ایمن کنید

VPN نرم‌افزاری است که به شما امکان می‌دهد، یک تونل امن میان کامپیوتر یا گوشی هوشمندتان و یک سرور که در هر نقطه‌ای می‌تواند باشد، (بهتر است که در یک کشوری که اینترنت نه سانسور شده است و نه کنترل می‌شود)، ایجاد کنید. این نرم‌افزار به شما امکان می‌دهد که از فیلترینگ و مسدودسازی عبور کنید. تمام

داده‌های ارسال شده از طریق این تونل رمزنگاری می‌شوند. VPN این اطمینان را به کاربران می‌دهد که در صورت انجام دستکاری مخرب (جاسوسی، تجاوز و غیره) بین کامپیوتر شما و سرور، این داده‌ها برای افراد ثالث قابل دسترس نباشند.

VPN علاوه بر اینکه امکان عبور از مسدودسازی را فراهم می‌کند، به شما امکان حفاظت از تمام اتصالات خروجی کامپیوتر را می‌دهد. اینگونه گردش شما بر روی اینترنت، اتصال به ارائه‌دهنده خدمات ایمیل ، دسترسی به فایل‌ها در خدمات ابری و غیره، تمام ترافیک اینترنت شما از طریق تونل ایجاد شده توسط VPN حرکت می‌کند و به چشمان کنجکاوان، اینترنت وای فای عمومی، ارائه‌دهنده خدمات اینترنت شما یا هر حمله و تجاوز دیگری از نوع مرد میانی قابل دسترسی نخواهد بود. ترافیک شما رمزنگاری شده تا سرور VPN و توسط این سرور رمزگشایی شود.



استفاده از VPN در مرورگر

تمرین:

1. نرم‌افزار VPN Nothing2Hide را بر روی کامپیوتر و گوشی هوشمند خود نصب کنید با دنبال کردن
2. راهنمای نصب راهنمای نصب ترجمه شود **lien installation VPN**

2. به https://www.whatismyip.net/ بروید.

3. VPN را فعال کنید و به https://www.whatismyip.net/ بازگردید و نتایج را مقایسه کنید.

حفاظت از اتصال و هویت با استفاده از Tor

هرچند با استفاده از یک VPN، گردش شما در اینترنت رمزنگاری می‌شود، اما به معنا آن نیست که شما ناشناخته هستید. حتی با یک VPN، شما نشان‌های زیادی از خود در آنلاین جا می‌گذارید، و نه تنها آدرس معرف به IP شما که اثر انگشتی دیجیتال شماست.

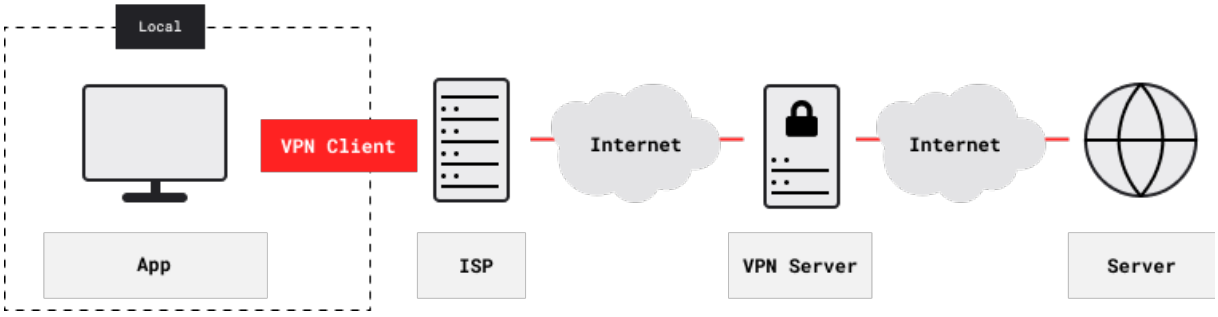
IP مخفف Internet Protocol است و کد یا آدرسی است که به دستگاه‌های متصل به اینترنت اختصاص داده می‌شود.

- این اثر انگشت همه‌ی نشانه‌های فنی کامپیوتر یا گوشی هوشمند شماست. از آن میان :
- مرورگر مورد استفاده (chrome, safari,)
- شماره نسخه آن
- سیستم عامل کامپیوتر شما ویندوز و یا ....
- زبان مورد استفاده شما
- یا ساعات مورد استفاده حتا اگر ساعت در مکان جغرافیایی دیگر باشد.

تمرین

شما می‌توانید با استفاده از وب‌سایت https://www.amiunique.org/ می‌توانید به گونه آنلاین اثر انگشت دیجتالی خود را ببینید.

مرورگر تور

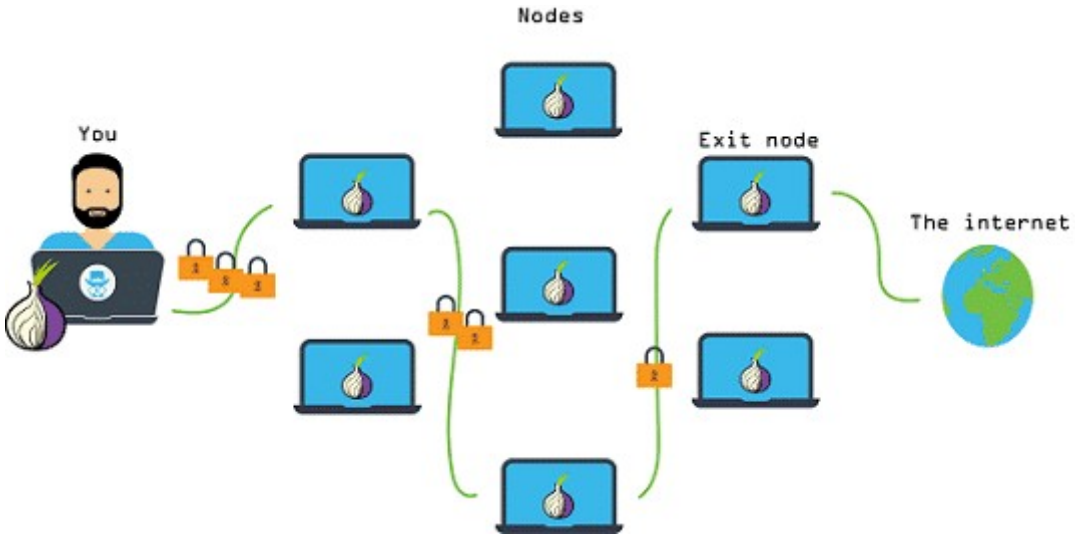


برای تقویت ناشناس ماندن خود در اینترنت، شما می‌توانید از مرورگر Tor استفاده کنید. مرورگر Tor سعی می‌کند گردش کاربران به نظر یکسان بیایند، تا نظرداشت و تعقیب شما با اثر انگشت دیجیتال اختصاصی مرورگر و اطلاعات دستگاه شما سخت‌تر شود.

علاوه بر این، برخلاف VPN که مدیران VPN ممکن است همزمان بدانند از کجا و به کجا وصل می‌شوید و این‌گونه ناشناس ماندن شما با چالش مواجه شود، Tor با ایجاد ناشناسی در شبکه امکان نمی‌دهد که نقطه مبدا و مقصد یک اتصال دانسته شود.

اگر کسی برعادات گردشگری شما بر روی اینترنت نظارت کند، تنها می‌تواند ببیند که شما از Tor استفاده می‌کنید.

Tor یا یک VPN همیشه شما را به صورت کامل ناشناس نمی‌کند. برای مثال، وقتی با یک VPN یا Tor به حساب فیسبوک خود با نام و نام خانوادگی وصل می‌شوید، این به معنای نقض ناشناس بودن شما است.



Tor بر روی کامپیوتر، ویندوز، مک، لینوکس، اندروید و آیفون قابل دسترسی است.

تمرین:

۱- Tor را با مراجعه به https://www.torproject.org/fa/download/ نصب کنید.

۲- به amiunique.org با استفاده از Tor و مرورگر روزانه‌ی خود بروید و نتایج را مقایسه کنید.

۳- به https://www.iplocation.net/find-ip-address با استفاده از Tor و مرورگر روزانه‌ی خود بروید و نتایج را مقایسه کنید.

۴- بر روی آیکون  در سمت چپ نوار آدرس کلیک کنید و مسیر Tor را بررسی کنید.

5. بر روی آیکون  در بالای صفحه کلیک کرده و تمام داده‌های بازدید فعلی را پاک کرده و یک صفحه جدید را گشوده کنید.

برای دانستن بیشتر:

- از یک سیستم‌عامل در فلش ، برای حفاظت از حریم خصوصی استفاده کنید: Tails.

- برای دانستن بیشتر دوره Totem آنلاین (به زبان فارسی) را دنبال کنید.