ایمنی در فعالیت آن‌لاین

- موضوع درس‌نامه : دستیابی به اطلاعات شخصی و خصوصی که از ما در فضای مجازی منتشر شده است، یادگیری حذف این اطلاعات. ایمن‌سازی، راهبرد جداسازی داده‌ها

https

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

آیا می‌دانید اصافه کردن حرف **s** در پایان این پروتکل اینترنتی به چه معناست؟

آیا به نام سازنده آن یعنی شرکت **S**afran است؟

آیا حرف جمع در زبان انگلیسی است؟

آیا به معنای **Secure** یا امنیت است؟

پاسخ درست : به معنای Secure یا امنیت است

https

یادآوری : (HTTPS) پروتکل امن انتقال ابرمتناست و ترکیبی از پروتکل HTTP و SSL است. هدف آن فراهم آوردن ارتباطات امن رمز شده و شناسایی امن یک کارگزار وب است.

https

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

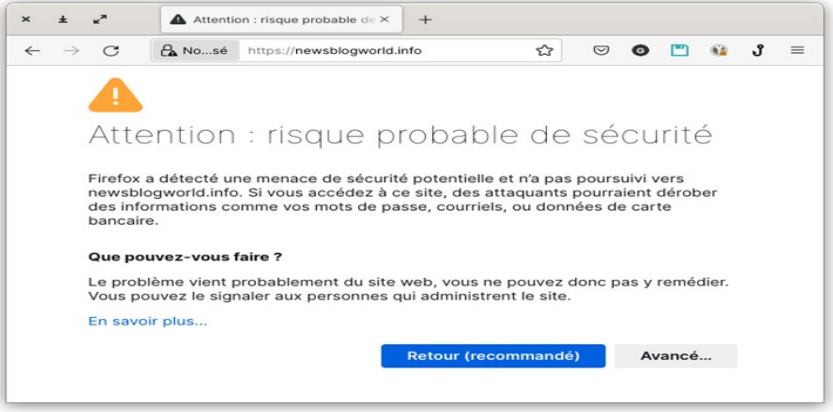
- **اعتبارو واقعی بودن وب‌سایت** : هر وب‌سایت با پروتکل https دارای یک گواهی ایمنی (certificat) است، به هنگام بازدید از آن مرورگر شما به آن دسترسی خواهد یافت. مرورگر شما دارای یک پایگاه داده‌ها است که امکان بررسی اعتبار این گواهی را دارد. این گواهی معادل کارت شناسایی وب‌سایت است و هر وب‌سایت به صورت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



بهتر کردن ایمنی آنلاین

برای استفاده درست‌تر از HTTPS از طریق مرورگر خود، مراحل زیر را دنبال کنید:

- از مرورگرهای Firefox، IE Edge یا Chrome استفاده کنید.
- از Évitez Microsoft Edge استفاده نکنید.
- افزونه Privacy Essentials Duck Duck Go را بر روی Firefox یا Chrome نصب کنید.
- برای استفاده در Android و iOS، از مرورگر Duck Duck Privacy Browser استفاده کنید.

تمرین

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

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

برای نصب افزونه اینجا را ببینید

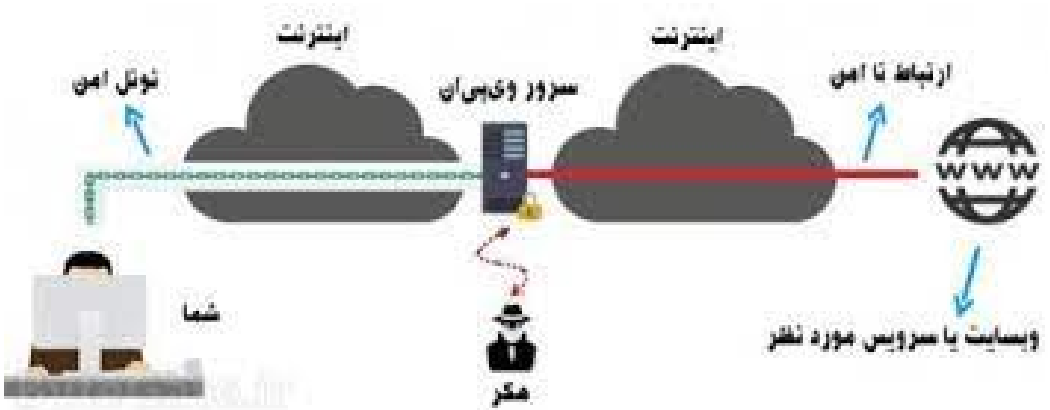
شنود و رصد داده‌ها

شنود و رصد داده‌ها

* 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



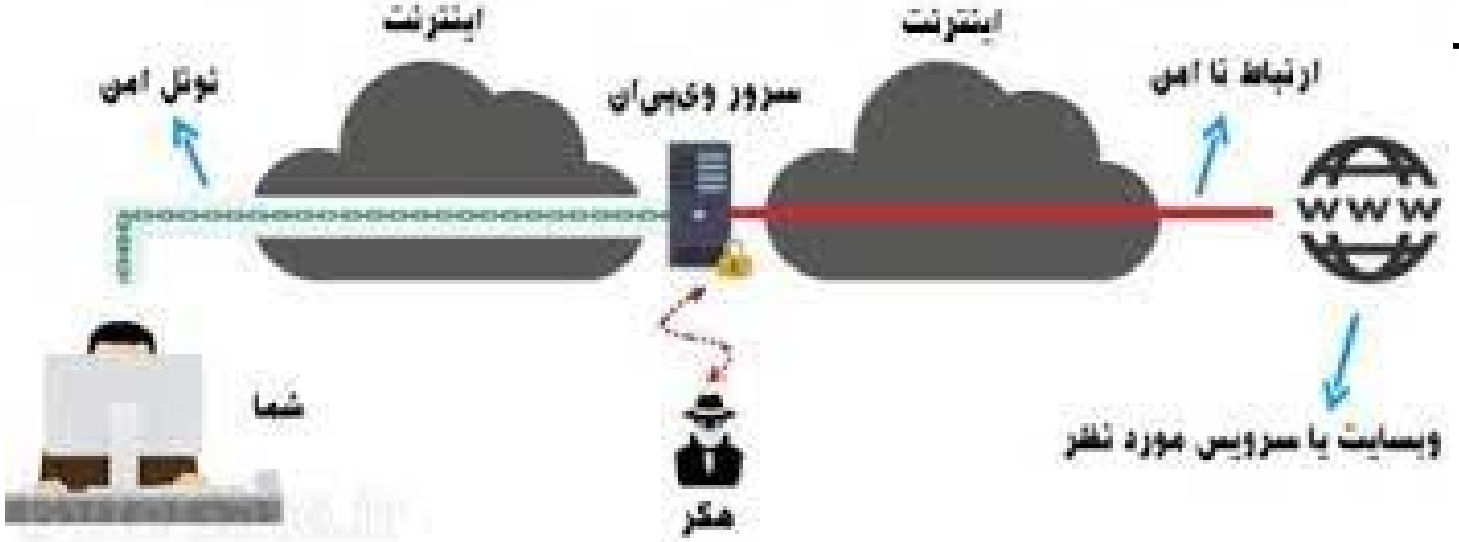
VPN نرم‌افزاری است که به شما امکان می‌دهد، یک تونل امن میان کامپیوتر یا گوشی هوشمندتان و یک سرور که در هر نقطه‌ای می‌تواند باشد، ایجاد کنید. این نرم‌افزار به شما امکان می‌دهد که از فیلترینگ و مسدودسازی عبور کنید.

VPN این اطمینان را به کاربران می‌دهد که در صورت

با VPN اتصال خود را ایمن کنید

VPN افزون بر فراهم آوردن امکان عبور از مسدودسازی، به شما این امکان را می‌دهد که تمام اتصالات خروجی کامپیوتر شما حفاظت شوند.

VPN حرکت و گردش شما در اینترنت را ایمن و از چشمان کنجکاوان، اینترنت وای فای عمومی، ارائه‌دهنده خدمات اینترنت یا هر حمله و تجاوز دیگری حفاظ



استفاده از VPN در مرورگر : تمرین

۱- نرم‌افزار VPN Nothing2Hide را بر روی کامپیوتر و گوشی هوشمند خود نصب کنید.

۲-به این آدرس
https://www.whatismyip.net بروید.

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

اثر انگشت رقمی

اگر گردش شما در اینترنت با استفاده از یک VPN رمزنگاری می‌شود، اما به این معنا نیست که بر روی اینترنت ناشناس هستید. حتی با یک VPN، شما هنوز نشان‌های زیادی از خود و به شکل آنلاین به 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.

اثر انگشت رقمی

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
- زبان مورد استفاده شما
- یا ساعات مورد استفاده حتا اگر ساعت در مکان جغرافیایی دیگر باشد.

تمرین

با این آدرس به سایت https://amiunique.org/

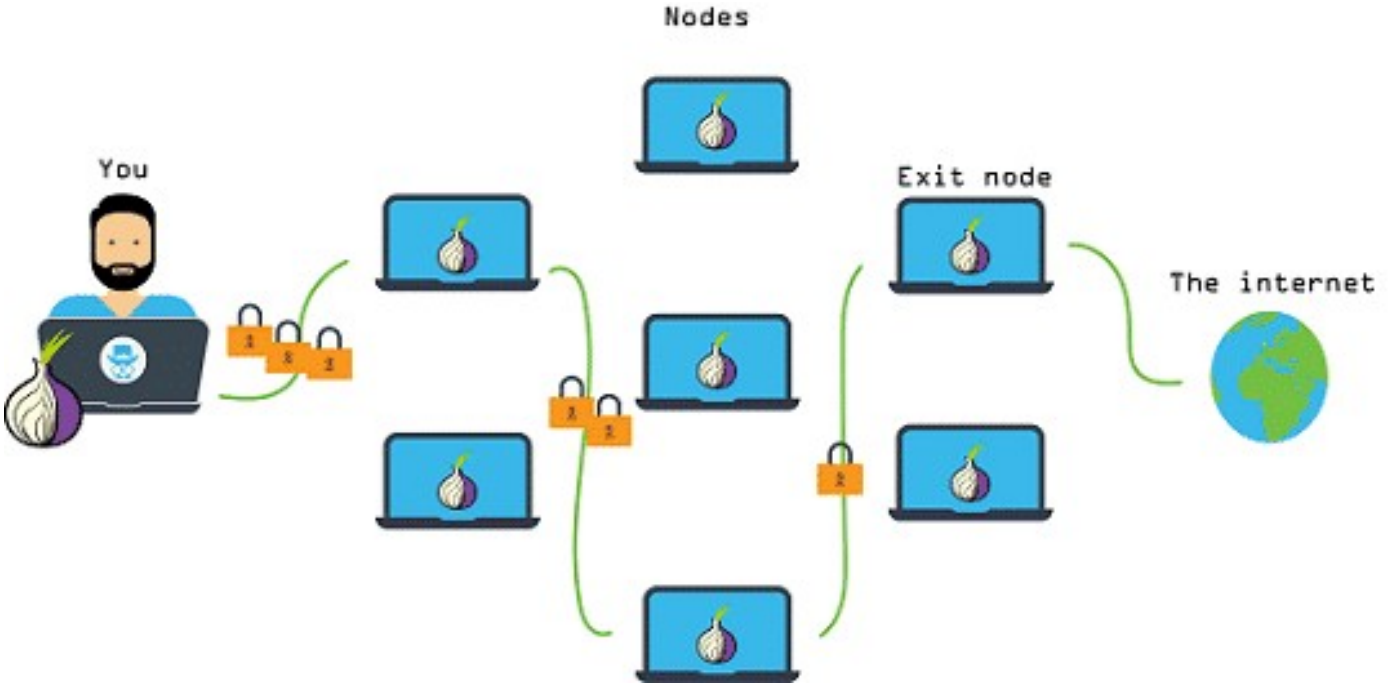
بروید و اثر انگشت‌های خود را ببینید!

حفاظت از گردش بر روی اینترنت و از هویت خود

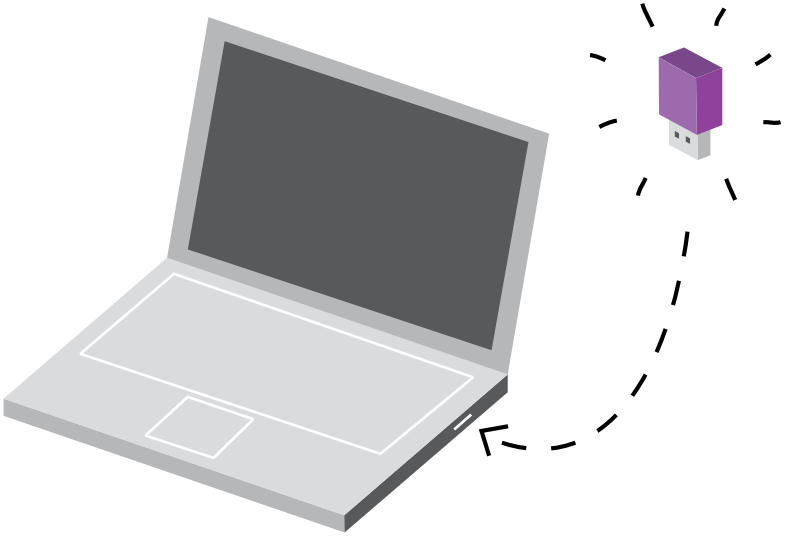
برای تقویت ناشناس ماندن خود در آنلاین، از مرورگر Tor استفاده کنید. مرورگر Tor سعی می‌کند تمام کاربران به نظر یکسان بیایند، تا نظرداشت و تعقیب شما با اثر انگشت دیجیتال منحصر به فرد مرورگر و اطلاعات دستگاه شما سخت‌تر شود.

علاوه بر این، برخلاف VPN که مدیران VPN ممکن است همزمان بدانند از کجا و به کجا وصل می‌شوید و این‌گونه ناشناس ماندن شما را با چالش مواجه می‌کند، 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.

حفاظت از گردش بر روی اینترنت و از هویت خود



برای دانستن بیشتر:



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