شبکه های اختصاصی مجازی

مقدمه

ممکن است برای شما پیش امده باشد که زمانی که از خانه دور هستید، مثلا زمانی که به یک رستوران و یا کافی شاپ می روید و یا در حال مسافرت نیاز داشته باشید تا از اینترنت بی سیم عمومی موجود در هتل و یا فرودگاه استفاده کنید. سوال اینجاست که چقدر این شبکه های عمومی امن هستند و چه کسانی فعالیت های آنلاین شما را تماشا و ضبط میکنند؟ شاید شما در خانه هم به سرویس دهنده اینترنت خود اطمینان نداشته باشید و بخواهید مطمئن باشید که آنها قادر نیستند فعالیت های آنلاین شما را نظارت کنند. در اینصورت میتوانید با استفاده از شبکه اختصاصی مجازی یا VPN (Virtual Private Network) از فعالیت های بر خط خود محافظت کنید. VPN به تکنولوژی اطلاق میشود که بوسیله آن میتوانید یک تونل اختصاصی و رمزگزاری شده ی امن برای فعالیت های آنلاین خود درست کنید تا با استفاده از آن امکان نظارت بر اعمال شما و مشاهده آن توسط دیگران بسیار سخت تر شود. علاوه بر این، با استفاده از VPN میتوانید با پنهان کردن محل زندگی خود باعث شوید وب سایت ها نتوانند به راحتی موقعیت شما را پیدا کنند.

چگونه کار میکند؟

VPN با ایجاد یک تونل اختصاصی و رمزگزاری شده به یک سرویس دهنده VPN که شما انتخاب میکنید کار میکند. کلیه فعالیت های شما از داخل این تونل به سرویس دهنده VPN شما رسیده و در نهایت از آنجا به مقصد مورد نظر شما می رسد. بعنوان مثال، اگر موقعیت فعلی شما در شهر تامپا از ایالت فلوریدا باشد و به یک سرویس دهنده VPN در مونیخ آلمان متصل شوید، کلیه سایتهایی که بازدید میکنید فکر خواهند کرد که شما از شهر مونیخ آلمان به آنها وصل شده اید. استفاده از VPN بسیار آسان است. قدم اول پیدا کردن سرویس دهنده ی مورد اطمینان و سپس درست کردن یک حساب کاربری برای خودتان است(برای این کار میباست سرویس مورد نظر را از آنها خریداری کنید). پس از اینکه حساب کاربری را درست کردید باید نرم افزار VPN را دانلود کرده و سپس نصب و پیکربندی کنید. بعد از نصب و پیکربندی به اینترنت وصل میشوید. نرم افزار VPN بدون اینکه شما متوجه چیزی بشوید تونل رمزگزاری شده را برای شما ایجاد کرده و از حریم خصوصی شما محافظت میکند.

انتخاب یک سرویس دهنده VPN

فعالیت های آنلاین شما تا زمانی امن و اختصاصی است که سرویس دهنده شما امن باشد.سرویس دهنده ای را انتخاب کنید که به آن اطمینان دارید. در ذیل نکات کلیدی را بررسی میکنیم که در انتخاب سرویس دهنده VPN به شما کمک میکند.

واقعه نگاری(Logging): بدنبال سرویس دهنده ای بگردید که هیچگونه گزارشی را نگهداری نکند و تمرکز آن بر روی حریم خصوصی باشد. اگر سرویس دهنده شما هیچگونه واقعه ای را جمع آوری و ثبت نکند، برای دیگران بسیار سخت خواهد بود تا متوجه شوند که شما چه فعالیتی داشته اید.

شرکت سرویس دهنده در چه کشوری قرار دارد: سرویس دهنده های مختلف در کشور های متفاوتی قرار دارند. اطمینان حاصل کنید که سرویس دهند ی شما در کشوری قرار دارد که قوانین حریم خصوصی در آنها بسیار قوی است. استفاده از سرویس دهنده هایی که در کشورهای با قوانین ضعیف در حوزه حریم خصوصی هستند ممکن است باعث شود تا از آنها بخواهند اطلاعات جمع آوری شده از شما را به آنها بدهند.

سرویس دهنده ها: از سرویس های VPN ای استفاده کنید که سرور های آنها در کشور و یا شهری هستند که شما نیاز دارید. بعضی از سرویس دهنده های VPN هزاران سرور در سراسر دنیا دارند. آیا شما نیاز دارید تا اتصال شما به اینترنت از کشور خاصی به نظر برسد؟ آیا آن شرکت امکان ارائه این سرویس را داراست؟

سازگاری: بدنبال سرویسی باشید که بتواند بر روی کامپیوتر های مختلف و تجهیزات همراه کار کنند. بعنوان مثال، سرویس VPN شما میبایست قادر باشد تا بر روی لپ تاپ ویندوز، تبلت و آیفون قابل استفاده باشد.

از سرویس های رایگان اجتناب کنید: در قبال استفاده از سرویس های رایگان بسیار محتاط باشید. چگونه آن سرویس دهنده ها میتوانند با ارائه سرویس رایگان به کسب و کار خود ادامه بدهند؟ سرویس های رایگان ممکن است اطلاعات شما را جمع آوری کرده و بفروش برسانند.

استفاده از VPN روشی فوق العاده برای محافظت از حریم شخصی شماست. با این حال، VPN نمیتواند کامپیوتر شما و یا اطلاعات حساب های آنلاین شما را امن نگه دارد. بنابراین اگر از VPN استفاده میکنید، حتما قدمهای اولیه برای امن نگه داشتن سیستم خود را فراموش نکنید، برخی از این قدمها شامل بروز رسانی دستگاه ها، قفل کردن صفحه کامپیوتر، استفاده از کلمات عبور قوی برای کلیه اکانت ها است.

سردبیر مهمان

فیل جانسی(@pearkreflections) فردی حرفه ای در تکنولوژی اطلاعات از شهر پالم بیچ کانتی و مجرب در حوزه امنیت، جرم شناسی رایانه ای(forensics) و ممیزی(auditing) میباشد. وی دارای مدرک جرم شناسی رایانه ای و مبانی امنیت از شرکت SANS بوده و بعنوان عضو هیئت مدیره انجمن OUTCH مشغول به کار است. علاقه و اشتیاق وی هرچه ساده تر کردن امنیت برای دیگران است.

منابع

ایجاد کلمات عبور ساده: https://www.sans.org/u/Sd8
امنیت تجهیزات همراه: https://www.sans.org/u/Sdd
بدافزار را متوقف کنید: https://www.sans.org/u/Sdi