پروتکل اتصال HTTPS چیست؟ و چه کاربردی دارد؟

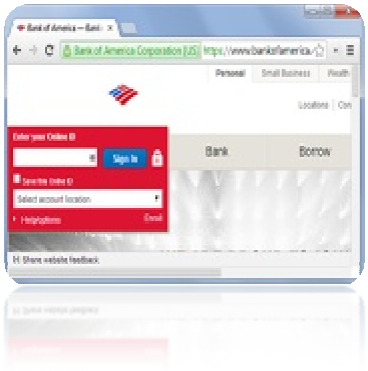
HTTPS در واقع همان آیکون قفلی است که در نوار آدرس مشاهده می‌کنید و اتصال به وب سایت ها را به صورت مطمئن و رمزگذاری شده برقرار می کند. استفاده از HTTPS مفهوم با اهمیتی است که در بحث هایی همچون خدمات آنلاین بانکی، خرید، اجتناب از فیشینگ و ... به کار می رود.

زمانی که شما به وب سایت های مختلف متصل می شوید، مرورگر شما از پروتکل استاندارد HTTP برای برقراری این اتصال استفاده می کند. HTTPS همتای رمزگذاری شده HTTP است و در واقع مخفف عبارت HTTP Secure است. نام این پروتکل به صورت کامل Hypertext Transfer Protocol Secure و به عبارتی دیگر پروتکل انتقال ابرمتن امن است.

زمانی که شما با استفاده از پروتکل HTTP به سایتی متصل می شوید، آدرسی که در مرورگر شما نمایان می شود همان آدرس وب سایت است و به نظر می رسد که به وب سرور اصلی متصل شده اید. در طول اتصال داده ها به صورت واضح بر روی شبکه که ارائه دهنده خدمات اینترنت است، فرستاده می شوند. اما تصور کنید که این اتصال به وب سایتی همانند وب سایت اصلی صورت گرفته باشد و از سوی دیگر شبکه شنود و مشاهده سیستم، صورت می گیرد بدون آن که شما از چیزی خبر داشته باشید. این مسئله از جمله مشکلات بزرگ پروتکل HTTP است .

در صورتی که گرفتار شبکه ای پر خطر شوید بدون آن که از چیزی خبر داشته باشید دیگر هیچ امنیتی برای شما باقی نمی ماند چرا که ممکن است در این اتصالات با ارسال داده های مهم همچون کلمه عبور و شماره کارت اعتباری و داده های دیگر بپردازید. همچنین با استراق سمع های متعدد می توانند از تمامی جستجوهای شما مطلع شوند.

به طور خلاصه HTTP هرگز اتصالات را رمزگذاری نمی کند و HTTPS با اضافه کردن رمزگذاری در تلاش برای حل این مشکل است.



HTTPSچگونه این مشکل را حل می‌کند؟

HTTPSکامل نیست اما مطمئنا بسیار امن تر از HTTP است. هنگامی که شما به یک سرور امن HTTPS متصل می شوید، زمانی که بخواهید سایت های امن مانند سایت

بانک خود را مشاهده و وارد آن شوید، به هنگام Log on کردن به صورت خودکار به سمت سرور HTTPS تغییر مسیر می دهید. در این حالت مرورگر شما نیز به بررسی موارد و گواهینامه های امنیتی پرداخته و تایید مجوز قانونی را جستجو می کند.

این پروتکل این اطمینان را به شما می دهد تا با مشاهده https://bank.com مطمئن شوید که به سایت واقعی و اصلی وصل هستید .اگر چه این پروتکل کامل نیست اما حضور آن مفید است. در نتیجه زمانی که شما به سایت مورد نظر خود Log onمی کنید و داده هایی همچون کلمه عبور و ... را ارسال می کنید، این داده ها به صورت رمزگذاری شده ارسال می شوند و این امر از استراق سمع افراد دیگر جلوگیری می کند.

HTTPSحریم خصوصی اضافی نیز فراهم می آورد. به عنوان مثال موتور جستجوی گوگل به صورت پیش فرض از اتصلات HTTPS استفاده می کند. این بدین معناست که افراد دیگر نمی توانند موارد جستجوی شما را در گوگل مشاهده کنند. در گذشته این طور بود که اگر افراد از یک شبکه یکسان Wi-Fi استفاده می کردند می توانستند حتی مقاله مورد مشاهده شما را نیز ببینند اما امروزه دیگر این امکان وجود ندارد یعنی اگر شما سایت ویکی پدیا را مشاهده کرده اید تنها می توانند این را بفهمند اما نمی توانند مقاله ای را که باز کردید را ببینند.

به طور خلاصه HTTP هرگز اتصالات را رمزگذاری نمی کند و HTTPS با اضافه کردن رمزگذاری در تلاش برای حل این مشکل است.

چگونه HTTPS در وب سایت‌هاشناسایی می‌شود؟

زمانی می توان گفت که با استفاده از اتصال امن به وب سایتی متصل شده اید که در نوار آدرس مرورگر خود https:// را به همراه آیکون قفل مشاهده کنید. همچنین برای کسب اطلاعات بیشتر می توانید بر روی more information کلیک کنید. شاید در مرورگرهای مختلف این روش متفاوت باشد اما همه مرورگرها در آیکون قفل و https://مشترک هستند .

هنگامی که شما باید مراقب باشید...

زمانی که می خواهید اطلاعات مهم ارسال کنید و یا این که به سایتی مهم وارد شوید، HTTPSبسیار با اهمیت است. زمانی که می خواهید اطلاعات خود را در سایتی وارد کنید حتما نوار آدرس خود را بررسی کرده که آیا HTTPS درج شده است یا نه. اگرچه این کار برای برقراری امنیت کافی نیست اما برخی از سایت ها که به دلیل کدگذاری نامناسب امن نیستند و به نوعی تهدید به شمار می آیند، توسط HTTPSشناسایی می شوند HTTPS .به دلیل آن که تایید هویت وب سایت را فراهم می کند با ارزش است.