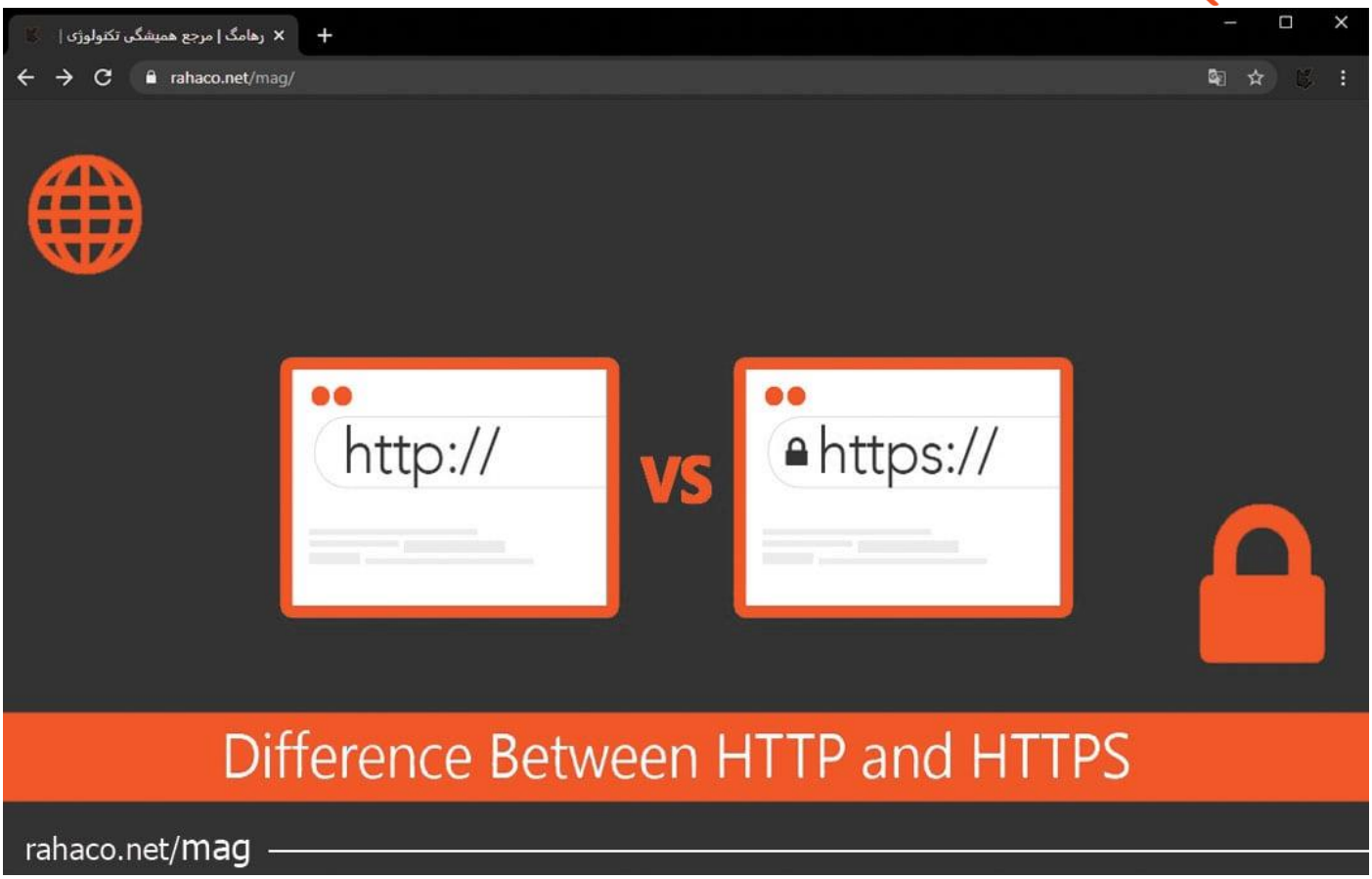
تفاوت HTTP و HTTPS در چیست و چگونه این پروتکل‌ها بر سئوی وبسایت تاثیرگذارند؟

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

مهم ترین تفاوت HTTP و HTTPS چیست؟

HTTP و HTTPS دو واژه‌ای هستند هر روز در دنیای اینترنت آن‌ها را می‌بینیم. در واقع، تغییر HTTP به HTTPS رتبه سئو سایت کاربر را در موتور جست و جوی گوگل افزایش می‌دهد؛ چرا که بیشتر بازدیدکنندگان معمولا از سایت‌هایی بازید می‌کنند که امنیت بیشتری داشته باشد. گوگل نیز اعلام کرد رتبه وبسایت‌هایی که از پروتکل https استفاده نمی‌کنند را کاهش می‌دهد.

HTTPS یک نسخه امنیتی پیشرفته از پروتکل انتقال hypertext یا ابرمتن است. از طرفی دیگر، HTTP پروتکل برنامه‌ای است که از طریق آن تمام ارتباطات داده در وب انجام می‌شود. HTTP به کاربران کمک می‌کند تا صفحات وب را بازیابی کنند. HTTPS یا HTTP Secure همین کار را انجام می‌دهد اما همانطور که از نامش پیداست، به شیوه‌ای امن‌تر. هنگام جستجو در فضای وب حتما یک URL را دیده‌اید: https://www.google.com

در این مقاله به بررسی تفاوت HTTP و HTTPS می‌پردازیم و اهمیت هرکدام از آن‌ها را شرح می‌دهیم.

HTTP چیست؟

HTTP مخفف Hypertext Transfer Protocol است که وظیفه اصلی آن انتقال داده‌ها در شبکه می‌باشد. HTTP از TCP (پروتکل کنترل انتقال) برای ارسال و دریافت داده‌ها از طریق وب استفاده می‌کند. به بیان ساده، HTTP پروتکلی است که توسط کلاینت و سرور استفاده می‌شود.

معمولا بیشتر صفحات وب از HTTP استفاده نمی‌کنند، زیرا روش امنی برای انتقال داده‌ها در یک شبکه نیست. این پروتکل اساسا برای وب سایت‌های قدیمی استفاده می‌شود.

دو نوع اصلی از پیام‌های HTTP

دو نوع اصلی از پیام‌های HTTP وجود دارد: درخواست و پاسخ. درخواست‌های HTTP توسط مرورگر و هنگام تعامل کاربر با صفحات وب ایجاد می‌شود. به عنوان مثال، اگر کاربر روی یک لینک کلیک کند، مرورگر یک سری درخواست "HTTP GET" برای محتوایی که باید در آن صفحه ظاهر شود، ارسال می‌کند. این درخواست به سرور مبدا یا سرور کش پروکسی می‌روند و در نهایت سرور یک پاسخ HTTP ایجاد می‌کند.

درخواست‌ها و پاسخ‌های HTTP در سراسر اینترنت به صورت متن ساده ارسال می‌شوند و مشکل اصلی آن همین است؛ همه می‌توانند این متن‌های ساده را بخوانند! این موضوع هنگامی اهمیت می‌یابد که کاربر بخواهد داده‌های حساس را از طریق یک وب سایت یا یک برنامه تحت وب ارسال کنند. در این صورت همه می‌توانند به رمز عبور، شماره کارت اعتباری یا داده‌های مهم شما دسترسی داشته باشند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

HTTPS چیست؟

HTTPS مخفف Hypertext Transfer Protocol Secure است که مسیر امن‌تری برای انتقال داده‌ها در بستر وب ارائه می‌دهد. به همین دلیل بیشتر وب سایت‌های امروزی از این پروتکل استفاده می‌کنند. معمولا سایت‌هایی که از طریق HTTPS کار می‌کنند، یک تغییر مسیر دارند، بنابراین حتی اگر "http :// " را تایپ کنید، برای تحویل داده به یک اتصال ایمن هدایت می‌شوید.

HTTPS همچنین از TCP (Transmission control protocol) برای ارسال و دریافت داده‌ها استفاده می‌کند و این کار را از طریق پورت 443 در یک اتصال رمزگذاری شده توسط لایه حمل و نقل امنیتی (TLS) انجام می‌دهد. داده‌های که با HTTPS ارسال می‌شوند، رمزگذاری می‌شوند تا بتوانند در مقابل تهدیدات و حملات ایمن بمانند. این پروتکل با رمز گذاری داده‌ها دیگر قابل خواندن نخواهد بود.

علاوه بر رمزگذاری ارتباطات، HTTPS برای احراز هویت دو طرفه در ارتباطات نیز استفاده می‌شود. احراز هویت به معنای تایید این است که یک شخص همان چیزی باشد که ادعا می‌کند. در HTTP، هیچ تایید هویتی وجود ندارد، اما در اینترنت مدرن، احراز هویت ضروری است. این امر از حملاتی مانند: ربودن DNS و جعل دامنه که در صورت عدم احراز هویت امکان پذیر می‌شود، جلوگیری می کند.

چرا HTTPS مهم است؟

هر سایتی که با اطلاعات امن سر و کار دارد، قطعا باید از HTTPS استفاده کند. حتی سایت‌هایی که آنچنان به طور خاص با داده‌های حساس سروکار ندارند، همچنان می‌توانند از این پروتکل بهره مند شوند. گوگل یکی از بزرگ‌ترین حامیان جستجوی ایمن HTTPS بوده است. تائو تران در سخنرانیBrightEdge's Share16، اظهار داشت که نشانی HTTPS برای اطمینان از ایمن بودن وبسایت‌ها، امری ضروری است.

تفاوت HTTP و HTTPS چیست؟

همیشه توصیه می‌شود که کاربران ا به دلایلی مانند: عملکرد بهینه، امنیت بیشتر و بهبود سئو سایت HTTPS از استفاده کنند. موارد دیگر تفاوت HTTP و HTTPS به شرح زیر است:

- HTTP نا امن است در حالی که HTTPS ایمن است.
- HTTP داده‌ها را از طریق پورت 80 ارسال می‌کند در حالی که HTTPS از پورت 443 استفاده می‌کند.
- HTTP در لایه برنامه عمل می‌کند، در حالی که HTTPS در لایه انتقال عمل می‌کند.
- HTTP به گواهی SSL نیاز ندارد، اما با HTTPS حتما باید یک گواهی SSL داشته باشید که توسط CA امضا شده باشد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

- HTTP نیازی به اعتبارسنجی دامنه ندارد، در حالی که HTTPS به اعتبارسنجی دامنه نیاز دارد و حتی برای گدریافت واهی‌های خاص به تایید اسناد قانونی نیاز دارد.
- در HTTP داده‌ها بدون رمزگذاری ارسال می‌شوند اما با HTTPS داده‌ها قبل از ارسال رمزگذاری می‌شوند.

لایه‌ها و URLهای OSI

یک تفاوت نهایی بین HTTP و HTTPS، لایه OSI و نحوه ساختار URLهای آن است. مدل OSI هفت لایه مختلف را نشان می‌دهد که ارتباط کامپیوترها از طریق آن‌ها برقرار می‌شود. این هفت لایه عبارتند از:

- لایه برنامه
- لایه ارائه
- لایه جلسه
- لایه حمل و نقل
- لایه شبکه
- لایه پیوند داده
- لایه فیزیکی

HTTP در لایه برنامه کار می‌کند و عمده فعالیت HTTPS در لایه انتقال است.

سئوی HTTP و HTTPS

سئو نیز در میان موارد تفاوت HTTP و HTTPS قرار دارد. از آن جایی که سایت HTTPS تمام داده‌ها را رمز گذاری می‌کند. به همین ترتیب، نه تنها از اطلاعات حساس کاربران مانند: رمز عبور و اطلاعات کارت اعتباری محافظت می‌شود، بلکه تاریخچه داده‌ها هم ایمن خواهد ماند.

ایجاد صفحات AMP

آخرین تفاوت HTTP و HTTPS که در این مقاله به آن اشاره می‌کنیم همین است. اگر کاربران بخواهند از AMP (صفحات شتابدار موبایل) استفاده کنند باید HTTPS داشته باشند. سرویس AMP گوگل به عنوان روشی برای بارگذاری محتوا با سرعت بسیار زیاد، بر روی تلفن همراه ایجاد شده است. محتوای AMP برای ایجاد تجربه کاربری بهتر در گوشی‌های هوشمند و تبلت ساخته و طراحی می‌شود. اگر ایجاد یک وب سایت سازگار با موبایل برای شما در اولویت است و با توجه به اهمیت روز افزون رتبه بندی جست و جوی موبایل و سئو، استفاده از پروتکل HTTPS ضروری است.

گواهی SSL چه کاربردی دارد؟

گواهی SSL اطلاعاتی را که کاربران در اختیار سایت قرار می‌دهند رمزگذاری می‌کند و در این صورت داده‌ها به یک کد تبدیل می‌شوند. حتی اگر کسی تلاش کند به داده‌های ارسال شده بین فرستنده و گیرنده دسترسی داشته باشد، به دلیل این کدگذاری،

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

قادر به درک آن نخواهد بود. علاوه بر این، HTTPS از طریق اضافه کردن لایه امنیتی TLS (امنیت لایه حمل و نقل) نیز ایمن می‌شود. TLS به یکپارچگی داده‌ها و جلوگیری از تغییر یا حذف آن‌ها کمک می‌کند.

کاربرد Cloudflare در HTTPS

هر وب سایتی که برای در سرویس Cloudflare ثبت نام کرده باشد می‌تواند HTTPS را فعال کرده و با یک کلیک پروتکل HTTP را از خود دور کند. این باعث می‌شود تا رمزگذاری TLS به طور گسترده‌ای در دسترس باشد تا از کاربران و داده‌ها در سراسر اینترنت محافظت کند.

نتیجه گیری

استفاده از رمزگذاری برای اتصال در سراسر اینترنت و برقرای ارتباطات شبکه داخلی سازمان بسیار مهم است. همانطور که گفتیم، گواهی SSL اصلی‌ترین تفاوت HTTP و HTTPS است. HTTP گواهی SSL ندارد، اما این مورد در پروتکل HTTPS موجود است که اطلاعات شما را رمزگذاری می‌کند تا اتصالات شما ایمن شوند. بنابراین، می‌توان گفت که HTTPS امن‌تر از HTTP است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net