HTTPS چیست ؟

HTTPS مخفف Hyper Text Transfer Protocol security است. یک پروتکل ارتباطی برای انتقال امن اطلاعات در شبکه‌های داخلی و اینترنتی و.روی پورت 443 است. بسیاری از سایتها امروزه به جهت پایین بودن امنیت آنها مورد حمله **هکر ها** قرار میگیرند و چهره آنها تغییر میکند و گاها وب سایت خسارتهای جبران ناپذیری میخورد اما HTTPS در بستر آن امکان رمزنگاری (Encrypt) و انتقال اطلاعات رمزنگاری شده فراهم می شود.

مزایای استفاده از HTTPS چیست ؟

1.حفظ امنیت اطلاعات در ارتباطات شبکه و اینترنتی

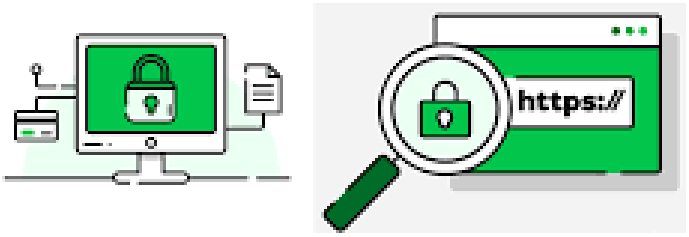
پروتکل https از دیده شدن اطلاعات و تغییر یافتن آن‌ها جلوگیری می‌کند. در صورت تغییر اطلاعات ارسالی از هر دو طرف، این تغییرات قابل شناسایی هستنداستفاده از

2. قابلیت های جدید مرورگر ها

نسخه‌های جدید مرورگرهای وب، برخی امکانات مانند دریافت اطلاعات مهم مثل مکان فیزیکی کاربر را تنها برای سایت‌هایی با پروتکل https فعال می‌کنند. سایت‌هایی که از سیستم http استفاده کنند، نمی‌توانند از تمامی امکانات جدید مرورگرها بهره‌مند شوند.

SSL چیست و کار آن چه میباشد ؟

زمانی که آدرس یک سایت را در مرورگر وارد می کنیم اطلاعات بین کامپیوتر ما و کامپیوتری که سایت روی آن قرار دارد (سرور) در حال رد و بدل هستند. پس اگر بتوانیم به طریقی ارتباط بین کامپیوتر خود و کامپیوتر سرور را امن کنیم اطلاعات ما دزدیده نخواهند شد. پروتکل SSL (**Socket Secure Layer**) یک استاندارد وب برای کدکردن اطلاعات بین کاربر و وب سایت است. اطلاعاتی که توسط یک اتصال SSL مبادله می شوند بصورت کد شده ارسال می شوند و بدین ترتیب اطلاعات مبادله شده از دزدیده شدن یا استراق سمع محافظت می شوند. SSL برای شرکتها و مشتریان این امکان را فراهم می کند که بتوانند با اطمینان اطلاعات خصوصی شان را به یک وب سایت بطور محرمانه ارسال کنند.



مزایای استفاده از SSL

بطور کلی گواهینامه های دیجیتال SSL دو مورد بسیار مهم زیر را در جهت تأمین امنیت ارتباط در شبکه فراهم می سازند:

اولین مورد رمز گذاری بسته های اطلاعاتی در هنگام تبادل آنهاست که این امکان را به سرویس دهنده و کاربر آن می دهد که ارتباط خود را در بستری امن و به دور از مداخله دیگران بصورت رمز شده و غیر قابل خوانش برای دیگران برقرار سازند و از صحت رد و بدل اطلاعات اطمینان حاصل کنند. بدون وجود این پروتکل، تمامی اطلاعات تبادل شده به سادگی توسط افراد ثالث در گره های (Node) بین راه قابل رویت، تغییر و سوء استفاده هستند.

مورد دوم تایید هویت وبسایت و یا سرویس نرم افزاری است که گواهینامه دیجیتال بروی آن نصب گردیده است. بدین معنی که مراجعه کننده به سایتی که دارای گواهینامه معتبر است می تواند از جعلی نبودن سایت و صحت هویت آن اطمینان حاصل کند و مطمئن باشد که سایت مذکور بر مبنای گواهینامه معتبرش واقعاً همان است که ادعا می نماید؛ نه یک سایت جعلی که شبیه به سایت اصلی ایجاد شده و با روشهای متعددی که برای انحراف مسیر و هک کردن وجود دارد کاربر را به سمت خود هدایت کرده است.