سازمان بورس و اوراق بهادار
Securities & Exchange Organization

بولتن آگاهی رسانی امنیت سایبری، شماره ۴

تفاوت HTTP و HTTPS؛ از نگاهی متفاوت

■ مرکز نظارت بر امنیت اطلاعات بازار سرمایه ■

تفاوت HTTP و HTTPS: از نگاهی متفاوت

زمانی که برای مراجعه به یک وب سایت، مرورگر خود را باز می‌کنید و نام سایت را وارد می‌نمائید، نکته‌ای که شاید کمتر به آن توجه کرده باشید، اضافه شدن کلمه http یا https به ابتدای آدرس ورودی شما است. تاکنون به این که این کلمه‌ها چه تفاوتی دارند و با استفاده از آن می‌توان به چه اطلاعاتی در مورد وب سایت مورد مشاهده خود دست یابید، فکر کرده‌اید؟

http://www.|

https://www.|

هنگامی که آدرس مربوط به یک وب‌سایت در مرورگر رایانه شما وارد می‌شود، اطلاعاتی بین رایانه شما و سرور وب سایت مربوطه (که در نقطه دیگری از کره زمین واقع شده)، بر روی بسترهای شبکه رد و بدل می‌شود. در صورتی که اطلاعات نام کاربری و رمز عبور خود را در سایتی وارد کنید، مقادیر نام کاربری و رمز عبور نیز بر روی همین بستر شبکه به آن سرور منتقل خواهد شد. بدیهی است این اقلام محرمانه (نام کاربری، رمز عبور و سایر اطلاعات ممکن) از میان سیستم های واسط متعددی در بستر شبکه اینترنت دست به دست شده و به مقصد می رسند. با توجه به وجود تجهیزات قوی و پیشرفته، همه چیز در کسری از ثانیه اتفاق می‌افتد و شاید چنین احساس نشود که یک کلیک شما، بسته اطلاعاتی می‌سازد و در چشم به‌هم زدن بین دهها تجهیز شبکه دست به دست شده و به سرور مقصد می‌رسد و پاسخ به درخواست شما نیز از سرور مقصد، از همین بستر شبکه گام به گام به سمت شما باز می‌گردد. هر یک از این سیستم‌های واسط در بستر شبکه در اختیار افراد، شرکت‌ها و یا سازمان‌های مختلف قرار دارد.

حال این پرسش به ذهن شما خطور می کند:

با این تفاسیر، آیا این افراد، شرکت‌ها یا سازمان‌ها می‌توانند اطلاعات محرمانه تبادل شده میان رایانه ما و سرور مقصد را مشاهده کنند؟

پاسخ: بله و به راحتی.

ابزارهای متعددی وجود دارد که امکان شنود اطلاعات تبادلی شما توسط آن تیم‌ها را فراهم می‌سازد.

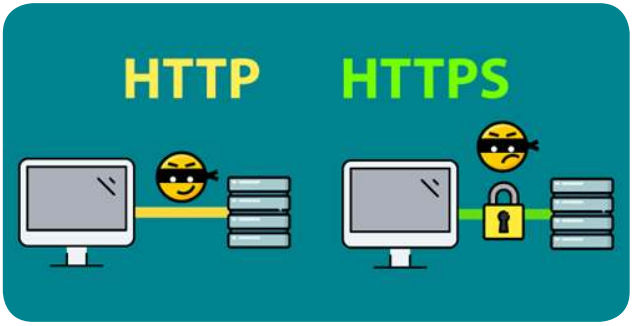
راهکار مقابله با مسئله چیست؟

پاسخ: رمزنگاری!

اما بدیهی است که افراد نمی‌توانند قابلیت رمزنگاری را در رایانه‌های خود برای یک سرور فراهم نمایند، بلکه باید سرور یا وب‌سایتی که به شما خدمات می دهد، امکانات لازم برای رمزنگاری داده های تبادلی میان رایانه شما و سرور خود را فراهم نماید.

https : راهکاری برای رمزنگاری

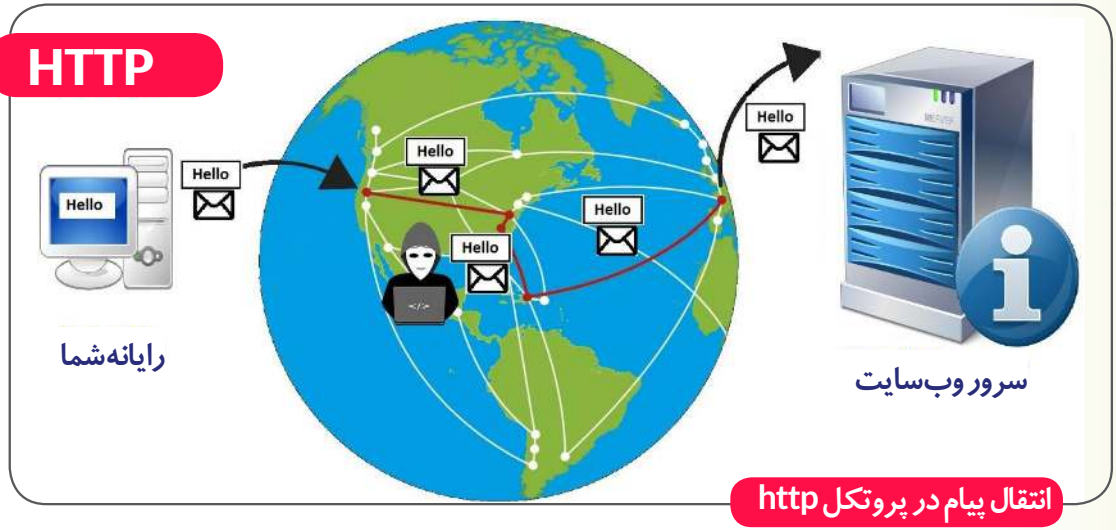
عبارات http و https که ممکن است در ابتدای آدرس وب سایت مورد نظر شما به طور خودکار اضافه شوند، پروتکل‌ها و قراردادهای تعریف شده و معینی برای تبادل اطلاعات شما با سیستم مقصد است. این پروتکل‌ها، نوع ارتباط و انتقال اطلاعات را مشخص می کنند. پروتکل http به معنای «پروتکل انتقال ابر متن» و پروتکل https به معنای «پروتکل انتقال **امن** ابر متن» است. در این مطلب، جزئیات فنی این دو پروتکل مورد بحث قرار نمی‌گیرند اما به صورت کلی نکاتی کاربردی در خصوص آن‌ها مطرح می‌شود.



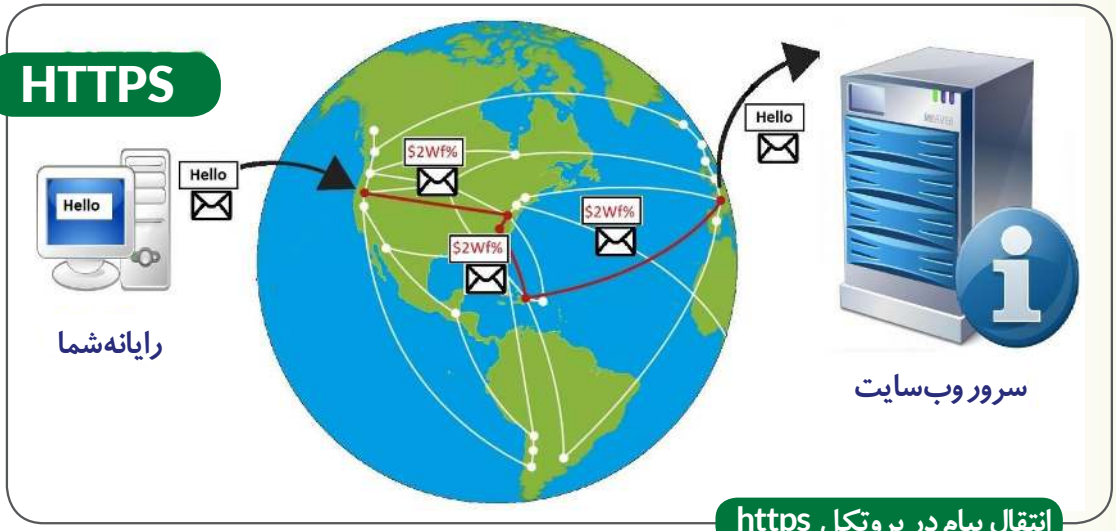
پروتکل https نسخه بهبود یافته و به اصطلاح امن پروتکل http است و قابلیت‌هایی برای انتقال امن اطلاعات شما فراهم نموده است. در پروتکل http اطلاعات ارسالی از سیستم شما به سیستم مقصد به صورت ساده و بدون اعمال مکانیزم‌های امنیتی و رمزنگاری منتقل می‌شود و سیستم‌های ارتباطی مابین سیستم شما و سیستم مقصد می‌توانند اطلاعات شما را به سادگی، شنود کنند. نام کاربری، رمز عبور، اطلاعات شخصی و هویتی و هرگونه اطلاعات تبادلی شما قابل شنود و سوء استفاده خواهد بود. در پروتکل https، بر خلاف پروتکل http اطلاعات به صورت ساده منتقل نمی‌شود بلکه اطلاعات شما ابتدا رمز شده و سپس بر روی بستر شبکه اینترنت ارسال می‌گردد. این مکانیزم موجب می‌شود که اطلاعات ارسالی شما در سیستم‌های میانی قابل شنود نباشد و عملا اطلاعات شما به شیوه امن‌تری منتقل می شود.

تفاوت HTTP و HTTPS به روایت تصویر:

در دو شکل زیر تفاوت نحوه انتقال اطلاعات در دو پروتکل http و https نشان داده شده است:



انتقال پیام در پروتکل http



انتقال پیام در پروتکل https

همانطور که در شکل‌های فوق نمایش داده شده است، پیام Hello ارسالی در پروتکل http به صورت ساده منتقل می‌شود و هکرها می‌توانند از طریق سیستم‌های واسط درون مسیر آن را مشاهده کنند، اما در پروتکل https این پیام به صورت رمز شده $2Wf% تبدیل شده و فقط برای سیستم‌های مبدا و مقصد قابل مشاهده است.

تشخیص وب‌سایت‌های http و https

برای تشخیص این که یک سایت از https استفاده می‌کند، در مرورگرهای مختلف بخشی از فضای مربوط به آدرس وب‌سایت به رنگ سبز در می‌آید و در برخی از مرورگرها علامت قفل سبز رنگی در کنار نام آدرس وب سایت نمایان می‌شود.

در شکل زیر، نشانه های https در مرورگرهای مختلف نمایش داده شده است:

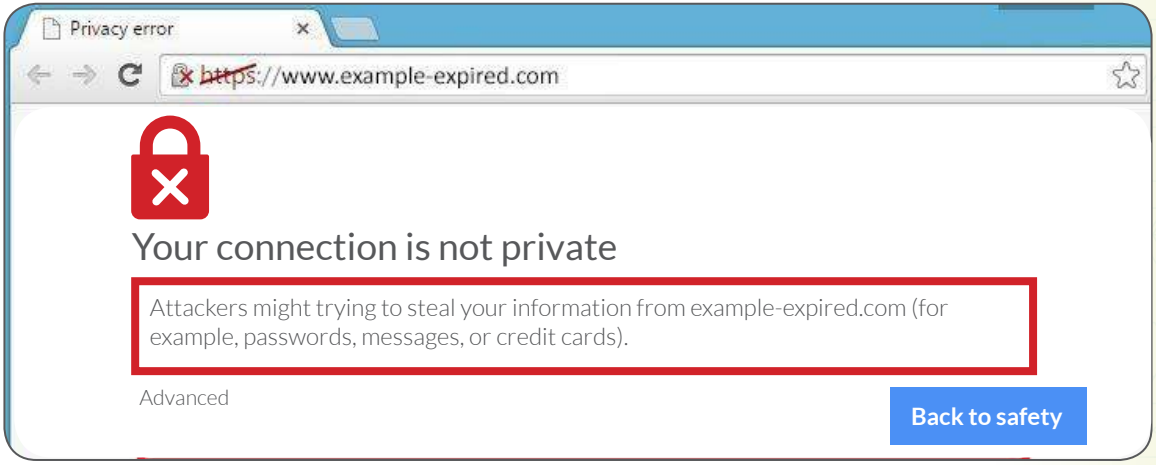
متاسفانه وب‌سایت‌های بسیاری وجود دارند که همچنان از پروتکل http استفاده می‌کنند و خطرات امنیتی در کمین کاربران آن سایت‌ها است.

چنانچه متوجه شدید در وب سایتی اطلاعات محرمانه شما بر روی شبکه منتقل می شود، در حالی که آدرس وب‌سایت https نیست، سعی کنید از مدیران یا متولیان وب‌سایت مورد نظر (اگر به آن‌ها دسترسی دارید) بخواهید که از پروتکل https استفاده کنند و سرویس‌دهی بر بستر پروتکل http را متوقف نمایند. این اقدام شما، به فرهنگ‌سازی ارائه سرویس امن کمک خواهد کرد. در صورتی که در وب سایت های مرتبط با بازار سرمایه چنین موردی را مشاهده نمودید، از طریق ایمیل makna@seo.ir به مرکز نظارت بر امنیت اطلاعات بازار سرمایه اطلاع دهید.

نکاتی در خصوص https

برای تبدیل یک وب‌سایت از http به https، نیاز است که مدیر یک وب سایت گواهینامه SSL را از محل‌های معتبری خریداری نموده و بر روی وب سایت خود این گواهینامه را پیاده سازی کند.

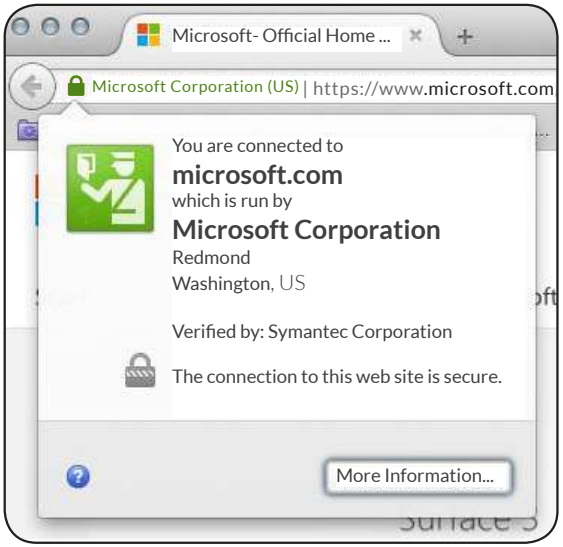
این گواهینامه‌ها تاریخ انقضاء دارند و در صورتی که منقضی شوند، پیام خطایی شبیه پیام زیر برای کاربر نمایش داده می‌شود:



البته نمایش پیام فوق علل دیگری نیز می‌تواند داشته باشد، در تمامی موارد می‌توان به اجرای صحیح و امن مکانیزم پروتکل https شک نمود!

بـه طـور کلـی پـس از وارد کـردن آدرس یـک وب‌سـایت در مرورگر اینترنت، با یکی از سـه حالت ذیـل مواجه خواهید شـد و تنها حالتی که انتقال امن اطلاعات شـما به سیسـتم مقصد فراهم می‌نماید، با رنگ سـبز مشـخص شـده اسـت:

در صورتی که بخواهید اطلاعات بیشـتری در خصوص پروتکل https اسـتفاده شـده و اعتبار گواهینامه خریداری شـده مرتبط در یک وب‌سـایت کسـب نمائید، بر روی آیکن سـبز رنگ مربوط به https کلیک کنید تا اطلاعات مربوط به آن را مشـاهده نمائید.



در اسـتفاده از وب‌سـایت‌های معاملات برخط بورسـی، وب‌سـایت‌های بانکی و وب‌سـایت‌هایی که اطلاعات شـخصی و مالی شـما در آن‌هـا وجـود دارد، حتمـا دقت نمایید که سـرویس‌دهی بر اسـاس پروتکل https باشـد.

توصیه های امنیتی ما را جدی بگیرید!

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شمـاره ۱۳، سازمان بورس و اوراق بهادار
صنـدوق پستـی: ۶۳۶۶-۱۹۹۳۵
تلفن: ۸۴۰۸۳۵۳۵-۰۲۱ makna@seo.ir

www.seo.ir