



https://www



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 می کنید و نام سایت را وارد می نمایید، نکته ای 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 کلمه ها چه تفاوتی دارند و با استفاده از آن می توان به چه اطلاعاتی در مورد وب سایت مورد مشاهده خود دست یابید، فکر کرده اید؟

 **https://www.|**

 **http://www.|**

وجود تجهیزات قوی و پیشرفته، همه چیز در کسری از ثانیه اتفاق می افتد و شاید چنین احساس نشود که یک کلیک شما، بسته اطلاعاتی می سازد و در چشم به هم زدن بین دهها تجهیز شبکه دست به دست شده و به سرور مقصد می رسد و پاسخ به درخواست شما نیز از سرور مقصد، از همین بستر شبکه گام به گام به سمت شما باز می گردد. هر یک از این سیستم های واسط در بستر شبکه در اختیار افراد، شرکت ها و یا سازمان های مختلف قرار دارد.

 هنگامی که آدرس مربوط به یک وب سایت در مرورگر رایانه شما وارد می شود، 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 می شود. 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

حال این پرسش به ذهن شما خطور می کند:

با این تفاسیر، آیا این افراد، شرکت ها یا سازمان ها می توانند 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 تبدالی شما توسط آن تیمها را فراهم می سازد.



راهکار مقابله با مسئله چیست؟



✓ پاسخ: رمزنگاری!

خدمات می دهد، امکانات لازم برای رمزنگاری داده های تبادل میان رایانه شما و سرور خود را فراهم نماید.

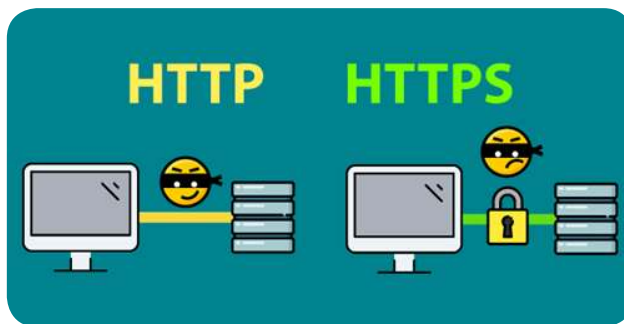
اما بدیهی است که افراد نمی توانند قابلیت رمزنگاری را در رایانه های خود برای یک سرور فراهم نمایند، بلکه باید سرور یا وبسایتی که به شما

https: راهکاری برای رمزنگاری



متن» و پروتکل https به معنای «پروتکل انتقال امن ابر متن» است. در این مطلب، جزئیات فنی این دو پروتکل مورد بحث قرار نمی گیرند اما به صورت کلی نکاتی کاربردی در خصوص آن ها مطرح می شود.

✓ عبارات http و https که ممکن است در ابتدای آدرس وب سایت مورد نظر شما به طور خودکار اضافه شوند، پروتکل ها و قراردادهای تعریف شده و معینی برای تبادل اطلاعات شما با سیستم مقصد است. این پروتکل ها، نوع ارتباط و انتقال اطلاعات را مشخص می کنند. پروتکل http به معنای «پروتکل انتقال ابر



اطلاعات تبدیلی شما قابل شنود و سوء استفاده خواهد بود. در پروتکل https، بر خلاف پروتکل http اطلاعات به صورت ساده منتقل نمی شود بلکه اطلاعات شما ابتدا رمز شده و سپس بر روی بستر شبکه اینترنت ارسال می گردد. این مکانیزم موجب می شود که اطلاعات ارسالی شما در سیستم های میانی قابل شنود نباشد و عملاً اطلاعات شما به شیوه امن تری منتقل می شود.

✓ پروتکل https نسخه بهبود یافته و به اصطلاح امن پروتکل http است و قابلیت هایی 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 مکانیزم های امنیتی و رمزنگاری منتقل می شود و سیستم های ارتباطی مابین سیستم شما و سیستم مقصد می توانند اطلاعات شما را به سادگی، شنود کنند. نام کاربری، رمز عبور، اطلاعات شخصی و هویتی و هر گونه

تفاوت HTTP و HTTPS به روایت تصویر:

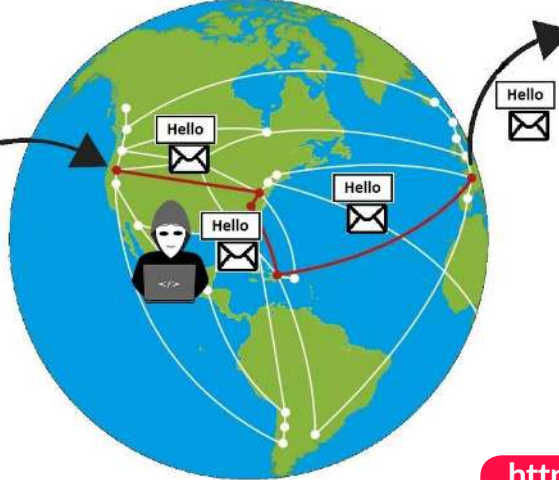


در دو شکل زیر تفاوت نحوه انتقال اطلاعات در دو پروتکل http و https نشان داده شده است: !

HTTP



رایانه شما



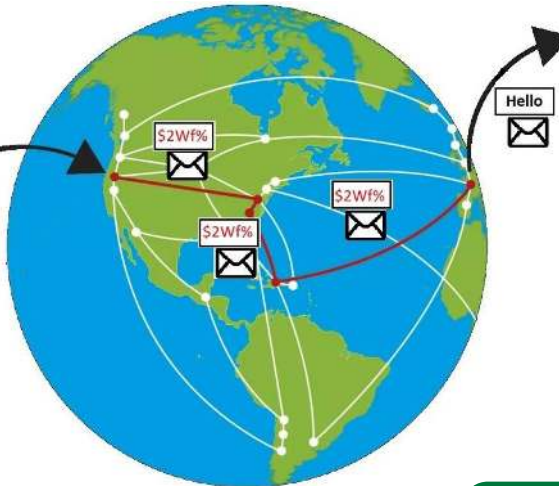
سرور وبسایت

انتقال پیام در پروتکل http

HTTPS



رایانه شما



سرور وبسایت

انتقال پیام در پروتکل https

اما در پروتکل https این پیام به صورت رمز شده $2Wf\$\%$ تبدیل شده و فقط برای سیستم‌های مبدا و مقصد قابل مشاهده است.

همانطور که در شکل‌های فوق نمایش داده شده است، پیام Hello اسالی در پروتکل http به صورت ساده منتقل می‌شود و هکرها می‌توانند از طریق سیستم‌های واسط درون مسیر آن را مشاهده کنند.

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 وبسایت نمایان می‌شود. در شکل زیر، نشانه‌های https در مرورگرهای مختلف نمایش داده شده است:



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

چنانچه متوجه شدید در وبسایتی اطلاعات محرمانه شما بر روی شبکه منتقل می‌شود، 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 وبسایت‌های 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.



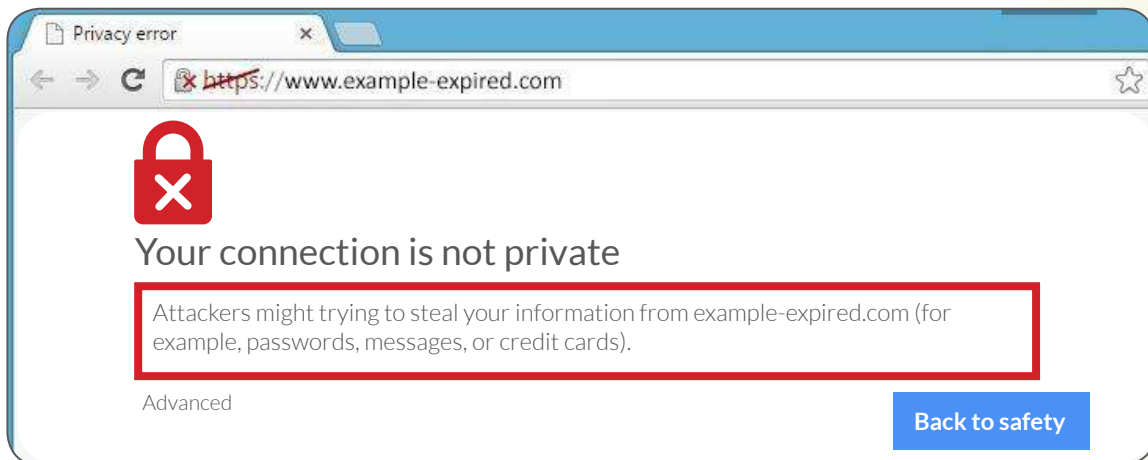
نکاتی در خصوص https



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



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

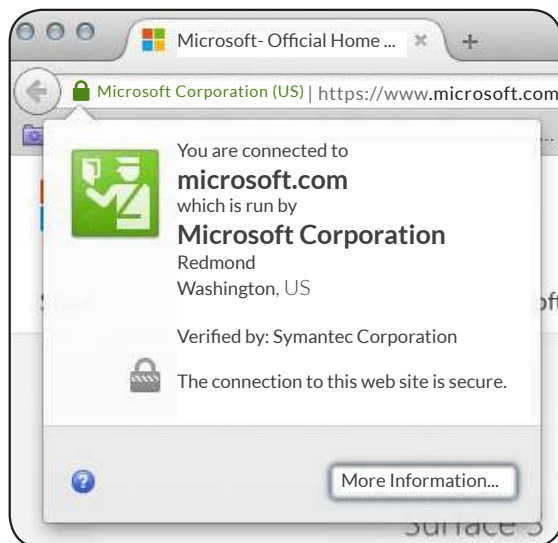


البته نمایش پیام فوق علل دیگری نیز می‌تواند داشته باشد، در تمامی موارد می‌توان به اجرای صحیح و امن مکانیزم پروتکل https شک نمود!

به طور کلی پس از وارد کردن آدرس یک وبسایت در مرورگر اینترنت، با یکی از سه حالت ذیل مواجه خواهید شد و تنها حالتی که انتقال امن اطلاعات شما به سیستم مقصد فراهم می‌نماید، با رنگ سبز مشخص شده است:



در صورتی که بخواهید اطلاعات بیشتری در خصوص پروتکل https استفاده شده و اعتبار گواهینامه خریداری شده مرتبط در یک وبسایت کسب نمایید، بر روی آیکن سبز رنگ مربوط به https کلیک کنید تا اطلاعات مربوط به آن را مشاهده نمایید.



در استفاده از وبسایت‌های معاملات برخط بورسی، وبسایت‌های بانکی و وبسایت‌هایی که اطلاعات شخصی و مالی شما در آن‌ها وجود دارد، حتما دقت نمایید که سرویس‌دهی بر اساس پروتکل https باشد.

توصیه‌های امنیتی ما را جدی بگیرید!
مرکز نظارت بر امنیت اطلاعات بازار سرمایه



مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شماره ۱۳، سازمان بورس و اوراق بهادار

صندوق پستی: ۶۳۶۶-۱۹۹۳۵

makna@seo.ir

تلفن: ۰۲۱-۸۴۰۸۳۵۳۵

www.seo.ir