

مشکل هشدار گواهی‌نامه‌ی SSL ، هنگام دسترسی به بعضی سایتها

پروتکل امنیتی لایه‌ی انتقال (Transport Layer Security) بر مبنای لایه‌ی سوکت‌های امن (Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است، بنا شده‌است. این پروتکل برای ایجاد یک لایه‌ی امنیتی هنگام انتقال داده‌ها در اینترنت، برای اهدافی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی و پیام‌های فوری اینترنتی به کار می‌رود. مطابق ...



پروتکل امنیتی لایه‌ی انتقال (Transport Layer Security) بر مبنای لایه‌ی سوکت‌های امن (Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است، بنا شده‌است. این پروتکل برای ایجاد یک لایه‌ی امنیتی هنگام انتقال داده‌ها در اینترنت، برای اهدافی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی و پیام‌های فوری اینترنتی به کار می‌رود. مطابق استاندارد نشانی‌های وب (URL) ها (که نیاز به یک ارتباط از نوع SSL دارند به جای http: با https: شروع می‌شوند).

در حال حاضر دو سامانه از سامانه‌های مبتنی بر وب در این دانشگاه، بر روی چنین لایه‌ای ارائه شده‌اند. سامانه‌ی سیدا (سامانه‌ی یک‌پارچه‌ی دانشگاهی ایران) و نیز سامانه‌ی خدمات ایمیل دانشگاه، با استفاده از سرویس‌دهنده‌ی ipSCA بر روی این پروتکل در اینترنت منتشر شده‌اند.

بعضی مرورگرها هنگام استفاده از این دو سامانه#پیام هشدار امنیتی را صادر می‌کنند که به پیام‌های آن‌ها در زیر اشاره می‌شود:

اینترنت اکسپلورر نسخه‌ی ۶:

Internet Explorer 6 -> Security Alert...The certificate was issued by a company that you have chosen not to trust...

اینترنت اکسپلورر نسخه‌ی ۸:

Internet Explorer 8 -> There is a problem with this website's security certificate.

فایرفاکس نسخه‌ی ۰/۳:

Firefox 3.0.x -> Secure Connection Failed mail.iaus.ac.ir uses an invalid security certificate.....

فایرفاکس نسخه‌ی ۵/۳:

Firefox 3.5.x -> This Connection is Untrusted You have asked Firefox to connect securely to login.libproxy.york.ac.uk, but we can't confirm that your connection is secure.....

آپرا نسخه‌ی ۱۰:

Opera 10.x -> Security Issue The certificate for "ipsCA Global CA Root" is signed by the unknown Certificate Authority....

سافاری:

Safari -> Safari can't verify the identity of the website "mail.iaus.ac.ir".

علت نمایش این پیام هشدار به‌طور خلاصه در انتهای همین مطلب توضیح داده شده است.

به کاربران گرامی توصیه می‌کنیم که به‌جای ایجاد استثناء و یا نادیده گرفتن هشدارهای گواهی، مرورگر خود را یا گواهی‌نامه‌ی جدید ipsCA به‌روزرسانی نمایند.

کاربران اینترنت اکسپلورر (Internet Explorer) ، گوگل کروم (Google Chrome) و سافاری (Safari) در محیط ویندوز باید به وب‌گاه به‌هنگام‌سازی ویندوز مراجعه نموده و وصله (قطعه‌ی به‌روزرسان) KB931125 که در نوامبر ۲۰۰۹ منتشر شده است را در ویندوز اعمال نمایند.

کاربران فایرفاکس (Firefox) مراحل زیر را دنبال نمایند:

- ۱ (در محیط فایرفاکس روی این لینک کلیک کنید.
- ۲ (در پنجره‌ای که با عنوان «Downloading Certificate» نمایش داده می‌شود گزینه «Trust this CA to identify web sites» را انتخاب و دکمه‌ی «OK» را کلیک کنید.
- ۳ (از فایرفاکس خارج شوید و مجدداً آن را اجرا نمایید. اکنون دیگر نباید پیام هشدار نمایش داده شود.

کاربران فایرفاکس (Opera) مراحل زیر را دنبال کنند:

- ۱ (در محیط آپرا روی این لینک کلیک کنید.
- ۲ (در پنجره‌ای که نمایش داده می‌شود، دکمه‌ی «» را کلیک کنید.
- ۳ (در پنجره‌ی بعدی، علامت گزینه‌ی «Warn me when using this certificate» را بردارید و دکمه‌ی «OK» را کلیک کنید.
- ۴ (دکمه‌ی «Install» را کلیک کنید.
- ۵ (افزودن گواهی‌نامه‌ی جدید را با کلیک روی «OK» تأیید کنید.
- ۶ (از آپرا خارج شوید و مجدداً آن را اجرا نمایید. اکنون دیگر نباید پیام هشدار نمایش داده شود.

** چرا این پیام هشدار صادر می‌شود؟

گواهی‌نامه‌های SSL در بسیاری از برنامه‌های کاربردی به‌عنوان ابزاری برای تأیید هویت یا اصالت از برنامه، کاربر و یا ماشین (رایانه یا سرور) استفاده می‌شود. بیش‌ترین استفاده از این گواهی‌نامه در

تأیید هویت وب سرورها برای اطمینان از یک عملیات مبتنی بر وب در محیط امن (https) به کار می‌رود. در اواخر دسامبر ۲۰۰۹ (بهمن ۱۳۸۹) شرکت ارائه‌دهنده‌ی خدمات لایه‌ی امن ipSCA – که ما از خدمات این شرکت برای تضمین دسترسی امن به وب‌گاه‌های دانشگاه استفاده می‌کنیم – اعلام کرد که مستندات جدید از این سرویس باید بر روی سرورهای ما نصب شود. این پرونده‌های گواهی‌نامه‌ی جدید، هنوز در به‌روزرسانی بعضی از مرورگرها از جمله فایرفاکس و آپرا اعمال نشده است. نتیجه این که کاربران این مرورگرها هنگام مشاهده‌ی وب‌گاه‌هایی که امنیت آن‌ها توسط ipSCA تضمین شده است، پیام هشدار عدم اعتبار گواهی‌نامه را مشاهده می‌کنند.

رفع مشکل باز نشدن سایت‌هایی که دارای گواهی‌نامه امنیتی (https) هستند

- [معرفی](#)
- [پسندها \(5 نفر\)](#)
- [بازدید \(۳۱۱ مرتبه\)](#)

حتما پیش اومده بعضی وقت‌ها که می‌خواین به سایت‌هایی که دارای گواهی‌نامه امنیتی معتبرن (https) برید با صفحه زیر مواجه می‌شوید



که در خط آدرس روی `https` که به رنگ قرمز در اومده یک خط کشیده شده است. در عنوان اخطار این صفحه می‌گه که گواهی امنیتی سرور هنوز معتبر نیست! در متن اخطار این نوشته بطور خلاصه می‌گه که شما سعی دارید به سایتی وصل بشید که گواهی امنیتی آن معتبر نیست و گوگل کروم نمیتونه تضمین کنه که این ارتباط مطمئن باشه و بعدش به ساعت و تاریخ فعلی سیستم شما اشاره داره و از شما می‌پرسه که این ساعت و تاریخ درست است اگر نه باید آن را اصلاح کنید و دوباره صفحه را باز کنید و به این ارتباط نا امن از طریق این صفحه فعلی ادامه ندهید. البته شما با فشردن گزینه `proceed anyway` میتونید به صفحه مورد نظرتون دست پیدا کنید اما معمولا صفحه بصورت نا امن و ناقص لود میشه و نمیتونید ارتباط موفق داشته باشید. نمونه اش سایت فیسبوک که به شکل زیر ظاهر میشه

فیس بوک

درخواست‌ها

-

پیام‌ها

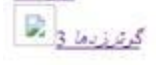
[Send a New Message](#)

پیام‌های دریافتی دیگر

-

نمایش پیام‌های پیشین

بین همه



ITPro.ir - انجمن تخصصی فناوری اطلاعات ایران

خوب شما خیلی راحت با به روز کردن زمان و تاریخ سیستم تان میتونید این مشکل رو حل کنید و صفحه مرور گرتونو دوباره باز کنید ویه ارتباط امن با ظاهر شدن https به رنگ سبز در خط آدرس داشته باشید .