در شش بخش گذشته از این سری مقالات، در خصوص امنیت مرورگرهای وب توضیح داده شد. در این قسمت به امنیت مرورگر اپل سافاری پرداخته می شود.

ویژگی های امنیتی سافاری

در نسخه (Mavericks) OS X 10.9 مرورگر سافاری، فلش پلیر همانند مرورگرهای IE، کروم و فایرفاکس در sandbox اجرا می شود. این ارتقاء امنیتی اپل سافاری به دلیل حفاظت در برابر بدافزارها می باشد و باعث می شود تا برنامه های خرابکار نتوانند در فایل ها بنویسند یا به داده های موجود در حافظه که توسط برنامه های کاربردی دیگر مورد استفاده قرار می گیرند دسترسی یابند. سایر پلاگین های خطرساز مانند Silverlight، QuickTime، جاوا و PDFها نیز در sandbox قرار گرفته اند و می توان اجازه دسترسی به سایت ها معتبر خاص را به برخی از پلاگین ها داد.

هم چنین در مرورگر سافاری، هر صفحه وب در یک پردازش مجزا اجرا می شود در نتیجه اگر کاربری وب سایتی را که در حال اجرای کد خرابکار باشد مشاهده کند، این عمل باعث از کار افتادن کل مرورگر نمی شود و آن برنامه خرابکار قادر نیست تا به داده های برنامه ها و صفحات دیگر دسترسی یابد.

مانند سایر مرورگرهای دیگر، مرورگر سافاری دارای حفاظت های حریم خصوصی تعبیه شده در مرورگر است. به عنوان مثال، کوکی های متفرقه به طور پیش فرض مسدود می شود و دسترسی وب سایت ها برای قرار دادن داده بر روی هارد درایو محلی مسدود می گردد. ویژگی "ردیابی نشود" وجود دارد و باعث می شود تا سایت ها نتوانند فعالیت های کاربر را ردیابی کنند. هم چنین مرورگر سافاری دارای یک مشخصه جستجوی خصوصی است که باعث می شود وب سایت های مشاهده شده به فهرست تاریخچه جستجو اضافه نگردند و اطلاعات جستجو و داده هایی که کاربر در فرم ها و وب سایت ها وارد می کند ذخیره نشود. مرورگر سافاری دارای نسخه قابل اجرا بر روی ویندوز نیز است.

پیکربندی امنیتی مرورگر سافاری

برای پیکربندی تنظیمات امنیتی در سافاری بر روی ویندوز، ابتدا باید گزینه Preferences از منوی ابزار (آیکون در سمت راست پنجره مرورگر) انتخاب شده و سپس Security انتخاب گردد. همانطور که در شکل ۱ مشاهده می شود تنها تعداد اندکی گزینه وجود دارد.

شکل ۱

به طور پیش فرض، تنظیمات امنیتی انتخاب شده در این صفحه باعث می شود تا هشدارهایی هنگام مشاهده وب سایت های کلاهبردار نمایش داده شود و قبل از ارسال فرم غیر امنیتی به یک وب سایت امن سوال پرسیده شود. به طور پیش فرض پاپ آپ ها مسدود می شوند. با این حال، باید توجه داشت پلاگین ها، جاوا و جاوا اسکریپت فعال می باشند، برای داشتن بهترین امنیت ممکن است کاربر برخی یا تمامی این گزینه ها را غیرفعال نماید.

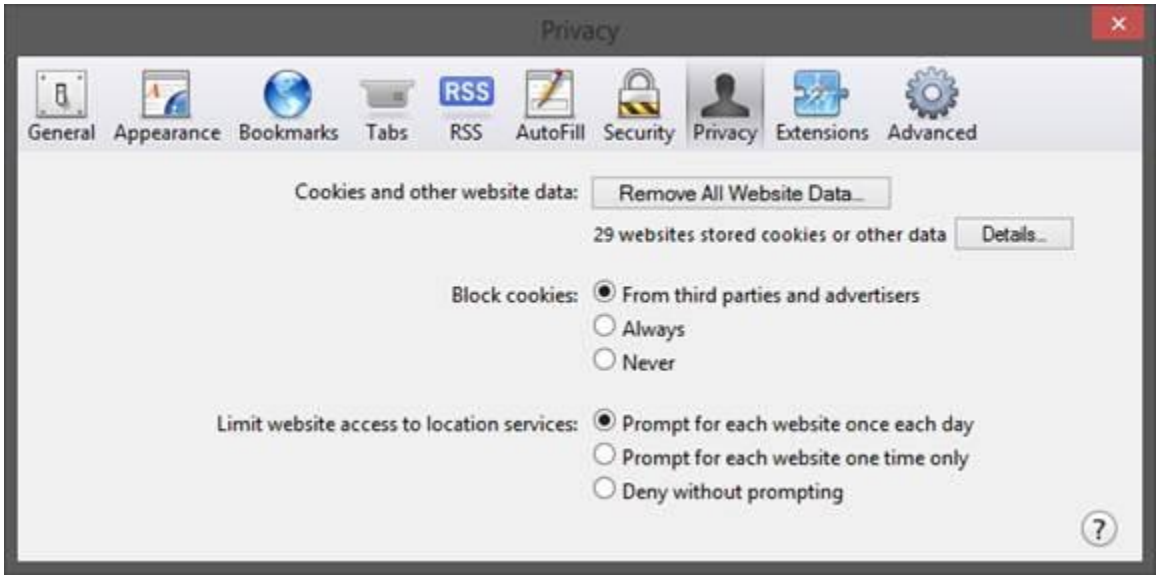
مرورگر سافاری بر روی سیستم عامل OS X کمی پیچیده تر است و همانگونه که در شکل ۲ مشاهده می گردد روبروی آیکون جاوا گزینهManage Website Settings قرار دارد.

شکل ۲

این گزینه به کاربر این امکان را می دهد تا وضعیت جاوا را بر روی وب سایت های مختلف کنترل کند. کاربر می تواند آدرس URL وب سایت هایی که می خواهد به آن ها اجازه دهد تا جاوا را اجرا نمایند را وارد نموده و با توجه به هر وب سایت یکی از چهار گزینه زیر را انتخاب نماید:

- Ask Before Using: با انتخاب این گزینه دیالوگ باکسی در هر زمان که سایتی می خواهد اپلت های جاوا را لود کند نمایش داده می شود. اگر نسخه به روز شده جاوا در دسترس باشد، کاربر را مجبور می کند تا ابتدا نسخه به روز شده را دانلود و نصب نماید.
- Block Always: با انتخاب این گزینه می توان اطمینان یافت که هیچگاه اپلت های جاوا اجازه اجرا ندارند.
- Allow: انتخاب این گزینه به سایت ها اجازه می دهد تا اپلت های جاوا را اجرا نمایند. اگر نسخه به روز شده ای از جاوا در دسترس باشد، کاربر را مجبور می کند تا ابتدا نسخه به روز شده را دانلود و نصب نماید.
- Allow Always: انتخاب این گزینه به وب سایت ها اجازه می دهد تا اپلت ها را بدون نیاز به دانلود و نصب آخرین نسخه از جاوا اجرا نمایند.

توجه: به دلیل کم بودن گزینه های امنیتی در سافاری، استفاده از این مرورگر در محیط های با امنیت بالا توصیه نمی شود به خصوص زمانی که بر روی سیستم های ویندوز در حال اجرا می باشد.
شکل ۳، گزینه Privacy را در تب Preferences نشان می دهد و در آن تنها چند گزینه ساده وجود دارد.



شکل ۳

می توان در این قسمت کوکی ها را حذف نمود، انتخاب نمود که چه زمانی کوکی ها مسدود شوند و هم چنین انتخاب نمود که چگونه سایت های وب می توانند به سرویس های محلی دسترسی یابند.

به نظر می رسد که مرورگر سافاری قابلیت مدیریت از طریق خط مشی گروهی را ندارد و تنها می توان از طریق خط مشی گروهی این مرورگر را بر روی ماشین های ویندوز غیرفعال کرد.

در قسمت آینده و آخرین قسمت از این سری مقالات به ویژگی های امنیتی اپرا پرداخته می شود.