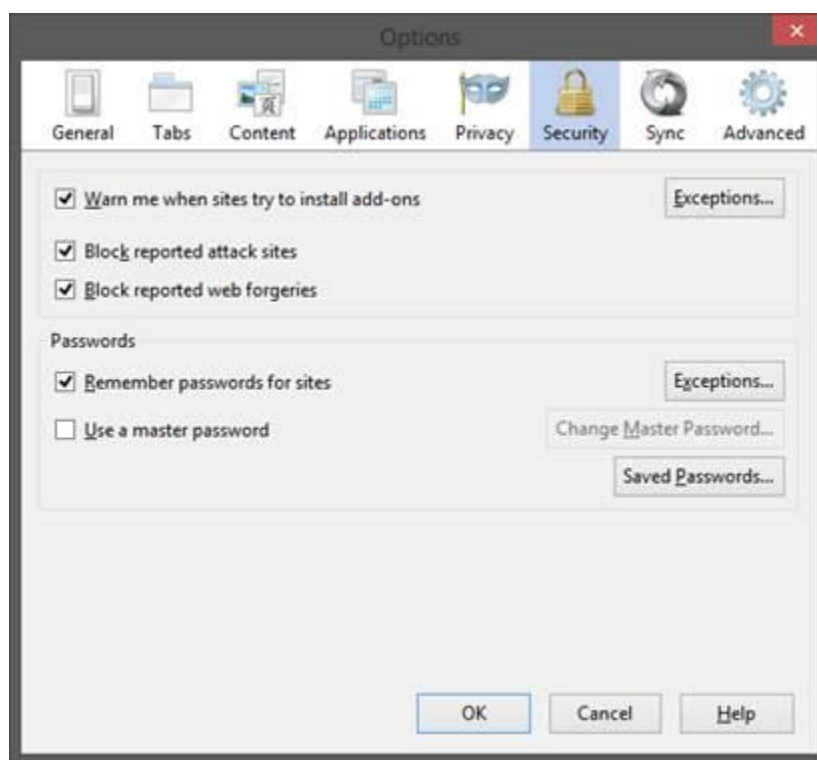


در مقاله پیشین مکانیزم های امنیتی مرورگر موزیلا فایرفاکس توضیح داده شد. در این قسمت تنظیمات امنیتی و ویژگی های حریم خصوصی مرورگر فایرفاکس تشریح می شود.

تنظیمات امنیتی

تنظیمات امنیتی فایرفاکس را می توان از طریق یک واسط گرافیکی انجام داد و می توان این تنظیمات را به گونه ای پیکربندی کرد تا سطوح مختلف امنیتی مرورگر در قبال عملیات مرتبط با امنیت را کنترل نمود. برای این منظور باید در نوار آدرس از پنجره مرورگر بر روی گزینه **Settings** کلیک کرده و سپس آیکون امنیت را از نوار بالای صفحه مطابق با شکل ۱ انتخاب نمود.



شکل ۱

در این صفحات گزینه ها به طور پیش فرض به گونه ای پیکربندی شده اند که بیشترین امنیت را فراهم نمایند. مرورگر فایرفاکس هنگامیکه افزونه ای در حال نصب باشد به کاربر هشدار می دهد و سایت های حمله گزارش شده و وب های جعلی خارجی را مسدود می کند. به کاربران توصیه می شود تا تنظیمات پیش فرض مذکور را تغییر ندهند. در صورتی که کاربر به سایتی اعتماد دارد و می خواهد این هشدارها را نادیده بگیرد می تواند از گزینه استثناء استفاده کرده و آدرس URL سایتی که به آن اطمینان دارد را ثبت کرده و در باکس مربوطه بر روی گزینه **Allow** کلیک نماید.

در این صفحه هم چنین می توان گزینه هایی مربوط به رمز عبور را مشاهده کرد و این قسمت جایی است که می توان با اعمال تغییراتی امنیت بهتری را فراهم کرد. به طور پیش فرض مرورگر فایرفاکس رمزهای عبور سایت ها را در حافظه نگه می دارد. اما برای داشتن امنیت بالاتر بهتر است تیک مربوط به این گزینه برداشته شود تا کاربر در هر بار اتصال به سایت مربوطه رمز عبور خود را وارد نماید.

اگر کاربر به فایرفاکس اجازه دهد تا رمزهای عبور را ذخیره نماید باید برای داشتن امنیت بهتر و حفاظت از فهرست رمزهای عبور از یک رمز عبور مستر استفاده کند. این گزینه به صورت پیش فرض فعال نیست اما می توان به راحتی این کار را انجام داد. کاربر باید مطابق شکل ۲، گزینه مربوط به **Change Master Password** را انتخاب کرده و رمز عبور مورد نظر را وارد نماید و از این طریق میزان سختی رمز عبور وارد شده سنجیده می شود.



شکل ۲

متاسفانه، مکان مخصوص وارد نمودن رمز عبور مستر حداکثر ۱۷ کاراکتر می باشد اما با ترکیب حروف الفبا، اعداد و سمبول ها می توان رمز عبور سخت تری را ایجاد کرد. پس از تنظیم این رمز عبور، کاربر باید قبل از برقراری هر نشستی که از رمز عبور ذخیره شده استفاده می کند، رمز عبور مستر را وارد نماید.

قابلیت های حریم خصوصی

همانند مرورگرهای IE و کروم، مرورگر فایرفاکس برای مقابله با ذخیره سازی اطلاعات تاریخچه جستجوها دارای گزینه های جستجوی خصوصی می باشد. تنظیمات مربوط به ردگیری و تاریخچه را می توان از طریق تب Privacy در دیاگنوسک Options پیکربندی کرد. هم چنین می توان به صورت دستی تاریخچه جستجوهای اخیر را حذف نمود. این تاریخچه شامل فهرستی از سایت های ملاقات شده، صفحات وب cache شده و کوکی ها می شود. به منظور پاک کردن تاریخچه، باید بر روی دکمه نارنجی Firefox در سمت چپ پنجره مرورگر کلیک کرد و سپس History | Clear Recent History را انتخاب نمود.

پیشگیری از ارتباطات خودکار

مرورگر فایرفاکس همانند مرورگرهای دیگر برخی اوقات به صورت خودکار برای به روز رسانی توصیفات ضد بدافزاری و ضد سرقت اطلاعات و اعمال اصلاحیه های امنیتی به اینترنت متصل می شود. هم چنین بدافزارها می توانند باعث شوند تا مرورگر به صورت خودکار به اینترنت متصل شود تا اطلاعات را برای مهاجم ارسال کنند.

در بسیاری موارد، می توان جلوی اتصالات خودکار را گرفت. به عنوان مثال می توان با حذف تمامی بوک مارک ها مانع از بارگذاری خودکار بوک مارک ها شد. اگر کاربری نمی خواهد هنگام بارگذاری صفحه اولیه به صفحه وب متصل شود می تواند صفحه اولیه blank را انتخاب کند. مرورگر فایرفاکس به صورت پیش فرض هر روز ابر داده های افزونه های نصب شده را به روز رسانی می کند. برای غیرفعال کردن این گزینه می توان `about:config` را در نوار آدرس تایپ کرد و کلید Enter را فشرد. سپس عبارت `extensions.getAddons.cache.enabled` را پیدا کرده و ارزش آن را به False تغییر داد.

خلاصه

در این مقاله به تشریح تنظیمات امنیتی مرورگر فایرفاکس پرداخته شد، در قسمت آتی بهترین تنظیمات امنیتی مرورگرهای اپل سافاری و اپرا شرح داده خواهد شد.