تنظیمات امنیتی

برای مرورگرهای کروم، اینترنت اکسپلورر و فایرفاکس

تدوین:

زهرا آیت

بسم الله الرحمن الرحیم .

مقدمه :

با سلام خدمت تمامی افرادی که این مطلب رو میخونن .
من زهرا آیت هستم و این مطالبی که مینویسم در جهت حفظ حریم خصوصی و امنیت کاربران ایرانی در استفاده از مرورگرها، نرم‌افزارها، و به طور کلی اینترنت است .
مطالب نوشته شده ترجمه تعدادی از مقالات انگلیسی در سایتهای مختلف، و همچنین تجربیات، مطالعات و بررسیهای شخصی خودم در زمینه‌ی امنیت میباشد .
کپی‌برداری این مطالب، با ذکر صلوات و انتشار عین این مقاله، در هر سایتی بدون هیچ محدودیت، برای همگان کاملا مجاز و رایگان میباشد .
این مطلب را در همه جا منتشر کنید تا امنیت سیستمهای خود و دیگران را در مقابل هکرها و باج‌افزارها به حداکثر برسانید .
این آموزش را به تمامی هموطنان عزیز ایرانی تقدیم میکنم .
امید که این کار مقبول درگاه الهی و استفاده‌ی شما هموطنان عزیز قرار بگیرد .

چکیده :

در این مقاله آموزشی به موارد زیر میپردازیم :
بهترین تنظیماتی که لازم است در مرورگرهایتان برای حفظ حریم خصوصی و امنیت خود انجام دهید،
نکات امنیتی عمومی که هر فرد لازم است برای حفظ اطلاعات شخصی خود و جلوگیری از دسترسی هکرها به آنها بداند،
توضیحاتی درباره برخی ویژگیهای جدید مرورگر فایرفاکس در نسخه‌های مختلف،
برخی مشکلات رایج در فایرفاکس که کاربران با آنها مواجه میشوند به همراه راهکار،
چند نکته‌ی امنیتی در استفاده از نرم‌افزارها و اینترنت
و همچنین جایگزینهای کدباز (opensource) برای برخی نرم‌افزارهای معروف پولی پر کاربرد .

❖ **راهکارهایی برای مرور امن در گوگل کروم (google chrome):**

تنظیمات google chrome برای حفظ حریم خصوصی و مرور امن در اینترنت:

این تنظیمات از طریق منوی تنظیمات پیشرفته‌ی chrome یا حرکت در chrome قابل دسترس است :

۱. **حفاظت در برابر فیشینگ (سارقان اطلاعات) و بدافزارها را فعال کنید :**

(Enable phishing and malware protection)

مطمئن شوید که ویژگی محافظت در برابر فیشینگ و بدافزارها در بخش تنظیمات حریم خصوصی (privacy settings) در Google chrome فعال است .

این ویژگی چنانچه سایتی که میخواهید از آن بازدید کنید، ممکن است سایت فیشینگ (سارق اطلاعات) یا دارای بدافزار باشد، به شما هشدار میدهد .

۲. **گزینه‌ی جستجوی سریع، (instant search) را خاموش کنید :**

ویژگی جستجوی سریع باید برای بهینه شدن امنیت خاموش باشد .

با این وجود که این ویژگی سهولت و راحتیهایی در جستجو برای شما فراهم میکند، اما فعال کردن این ویژگی بدین معنیست که هر چیزی که شما در نوار آدرس مینویسید، به سرعت برای گوگل ارسال میشود .

۳. **از همگامسازی (sync) استفاده نکنید :**

اتصال حساب ایمیل خود را در تب چیزهای شخصی از مرورگر قطع کنید .

همگامسازی حساب ایمیل شما با مرورگر وب کروم شما بدین معنیست که اطلاعات شخصی مانند: رمزهای عبور، اطلاعاتی که به صورت خودکار پر میشوند، تنظیمات و ... در سرورهای گوگل ذخیره میشود .

اگر حتما باید از sync استفاده کنید، گزینه‌ی رمزگذاری تمام اطلاعات همگام‌سازی شده ("Encrypt all synced data")را انتخاب کنید و برای رمزگذاری، عبارت عبور یکتایی انتخاب نمایید .

۴. **تنظیمات (content settings) را انجام دهید :**

بر روی گزینه‌ی "Content settings" در بخش (privacy) کلیک کرده و موارد زیر را انجام دهید :

۴,۱. کوکیها :

گزینه‌ی "Keep local data only until I quit my browser" and "Block third-party cookies and site data."را انتخاب کنید .

(نگه‌داشتن کوکیها و اطلاعات داخلی تا هنگامی که مرورگرم را قطع میکنم) و (کوکیهای شخص ثالث و اطلاعات سایت را مسدود کردن)

این گزینه‌ها به شما اطمینان میدهد که کوکیهای شما با قطع کردن مرورگر کروم پاک میشوند و تبلیغ کنندگان تجاری نمیتوانند شما را با استفاده از کوکیهای شخث ثالث، (third-party cookies) ردیابی کنند .

۴,۲. java script:

گزینه‌ی "Do not allow any site to run JavaScript." (به هیچ سایتی اجازه ندهید که جاوا اسکریپت را اجرا کند) را انتخاب نمایید .

این موضوع بطور گسترده توصیه میشود که جاوا اسکریپت تا جایی که امکان دارد غیر فعال باشد تا کاربران را از آسیب‌پذیریهای امنیتی آن، مصون بدارد .

۴,۳. پاپ آپ (pop-ups) :

"Do not allow any site to show pop-ups" تعیین کنید که به هیچ سایتی برای نشان دادن pop-ups (پنجره‌های تبلیغاتی ناخواسته) اجازه نده .

۴،۴. مکان:

"Do not allow any site to track my physical location" تعیین کنید که به هیچ سایتی برای ردیابی مکان فیزیکی من اجازه نده .

۵. تنظیمات فرمها و رمزهای عبور را انجام دهید :

"Offer to save passwords I enter on the web" (unchek autofill and passwords and form) غیر فعال کنید .

انجام این کار کروم را از ذخیره‌ی اطلاعات ورود به سیستم، رمزهای عبور و تمام اطلاعات مهم دیگری که در فرمها وارد میکنید، بازمیدارد .

❖ **راهنماییهایی برای مرور امن در موزیلا فایرفاکس (mozilla firefox):**

تنظیمات حریم خصوصی فایرفاکس :

این تنظیمات از طریق منوی options قابل دسترس است .

الف) تنظیمات حریم خصوصی را انجام دهید :

در تب تنظیمات privacy مراحل زیر را کامل کنید :

این مقادیر تضمین میکند که فایرفاکس، فقط آن مقدار اطلاعاتی را از شما ذخیره میکند، که برای درست کار کردن به آنها نیاز دارد .

۱. **برای تاریخچه‌ها، "Use custom settings for history." را انتخاب نمایید .**
"Remember my browsing and download history." را غیر فعال کنید، تا فایرفاکس، تاریخچه‌ی مرورها و دانلودها را ذخیره نکند.

۲. **"Remember search and form history." را غیر فعال کنید تا تاریخچه‌ی فرمها و جستجوهای شما را به خاطر نسپارد .**

۳. **"Accept third-party cookies." را هم غیر فعال کنید.**

۴. **نگهداری کوکیها را تعیین کنید فقطکوکیها تا زمانی باقی بمانند که فایرفاکس را میبندید .**

ب) تنظیمات امنیتی را نیز انجام دهید :

در تب security این موارد را انتخاب کنید :

این مراحل، فایرفاکس را از ذخیره‌ی رمزهای عبور شما بازمیدارد و شما را از بازدید سایتهایی که بالقوه خطرناک هستند، حفظ میکند .

۵. **بررسی کنید که :**

"Warn me when sites try to install add-ons"
"Block reported attack sites"
"Block reported web forgeries"

همگی فعال باشند .

این گزینه‌ها با نصب مرورگر، به صورت پیشفرض فعال هستند و نیاز به تغییر دادن آنها نیست.

این گزینه ها باعث میشوند فایرفاکس، هنگامی که یک سایت بخواهد افزونه‌ای بر روی مرورگر شما نصب کند، هشدار دهد .

همچنین وبسایتهای مهاجم و وبسایتهای جعلی را نیز مسدود کند.

دو گزینه‌ی آخر در فایرفاکس ۴۷ و قبلتر وجود دارد و در ورژن ۴۸ تغییراتی داشته و یک گزینه به آن اضافه شده است که آن نیز، به صورت پیشفرض فعال است .

Block dangerous and deceptive content
Block dangerous downloads

که وبسایتهای خطرناک یا فریبنده و همچنین دانلودهای خطرناک را مسدود میکند.

Warn me about unwanted and uncommon software.

گزینه‌ی جدیدی که به نسخه‌ی ۴۸ به بعد اضافه شده است، میباشد. بدین معنی که به شما موقع دانلود نرم‌افزارهای غیر متعارف و ناخواسته هشدار دهد. نرم‌افزارهای ناخواسته میتوانند حاوی کدهای خطرناک و مخرب باشند و بدین جهت، توصیه میکنم از فایرفاکس ۴۸ به بعد استفاده نمایید

گزینه‌ی به خاطر داشتن رمزهای عبور برای سایتها، "Remember passwords for sites.") در فایرفاکس ۴۷ به قبل، و Remember logins for sites در نسخه‌ی ۴۸ به بعد) را غیر فعال کنید .

۶. جاوا اسکریپت , (java script) را غیر فعال کنید :

در تبcontent ، "Enable JavaScript"را از انتخاب خارج کنید .

java scripts در داشتن آسیبپذیریهای امنیتی شناخته شده و زبانزد است و توصیه میشود که: کاربران فقط در صورتی که به سایتی اعتماد کامل دارند، آن را (فقط برای آن سایت،) فعال کنند .

فعال بودن این گزینه معمولا کاربرد چندانی ندارد و کاربرد آن مثلا در ایمیل و youtube است (.

توجه: (غیر فعال کردن java script در فایرفاکس ۲۳ به بعد، به تنظیمات پیشرفته فایرفاکس منتقل شده است که با نوشتن

about:config

در نوار آدرس قابل دسترس است .

درباره این گزینه در ادامه توضیحاتی ذکر میکنم (.

۷. بلاک کردن پنجرههای تبلیغاتی را فعال کنید :

اطمینان حاصل کنید که "Block pop-up windows" در تبcontent انتخاب و , فعال باشد .

این ویژگی به صورت پیشفرض روشن است، زیرا کاربران را از تبلیغات بیجا و پنجرههای (ناخواسته) محافظت میکند .

۸. از همگامسازی (sync) استفاده نکنید :

از استفاده از sync در فایرفاکس خودداری نمایید .

با انجام این کار، شما فایرفاکس را از ذخیرهی اطلاعات ورود به سیستم، رمزهای عبور و سایر دادههای مهم خود بازمیدارید .

۹. به روز رسانی خودکار، (automatic update) را فعال کنید :

بررسی کنید تا نصب به روز رسانیهای خودکار مرورگر، در تب update در تنظیمات , ".Advanced" انتخاب شده باشد .

انجام این کار، تضمین میکند که مرورگر شما، به روز رسانیهای امنیتی بسیار مهم و حیاتی را دریافت میکند .

همچنین بررسی کنید تا "Automatically update Search Engines" به روز رسانی خودکار موتورهای جستجو) نیز، انتخاب شده باشد (این گزینهها نیز به صورت خودکار، فعال هستند).

۱۰. از پروتکلهای امن استفاده کنید :

مطمئن شوید که: استفاده از "SSL 3.0 و "TLS 1.0در تب "Encryption" در تنظیمات ".Advanced"انتخاب شده باشد .

این گزینهها نیز در فایرفاکسهای جدید، به تنظیمات پیشرفته منتقل شده است، اما خوشبختانه به صورت پیشفرض فعال است .

❖ **راهکارهایی برای مرور امن با مرورگر internet explorer 10:**

این تنظیمات، از طریق منوی "Internet Options" قابل دسترس است .

❖ **الف) تنظیمات امنیتی را انجام دهید :**

۱. **در تب "Security" این موارد را تنظیم کنید :**

تنظیمات منطقه را انجام دهید :

اینترنت اکسپلورر، گزینه ای دارد که از طریق آن میتوانید تنظیمات امنیتی مختلفی برای نواحی مختلف، داشته باشید .

که شامل این موارد میشود :

شبکه گسترده‌ی جهانی، شبکه‌ی محلی، سایتهای مورد اعتماد و همچنین سایتهای ممنوعه و محدود شده .

Internet, local intranet, trusted sites و restricted sites.

تنظیمات منطقه ای را برای Internet, trusted sites و restricted sites مطابق با نیاز خودبراساس درجه‌ی امنیت، انجام دهید .

امنیت Internet zone security را "Medium High" یا higher تنظیم کنید .

این کار، انواع خاصی از کوکیها را مسدود میکند، فیلتر کردن (activex) را فعال میکند، و چندین تنظیم پیشفرض دیگر را برای افزایش امنیت، دارا میباشد .

۲. **javaScriptرا غیر فعال کنید :**

بر روی "Custom Level..." کلیک کرده، "Active Scripting" setting و انتخاب کنید تا غیر فعال (disable) باشد .

توصیه میشود که کاربران، JavaScriptرا به دلیل آسیبپذیریهای امنیتی زیادی که دارد، غیر فعال کنند .

۳. **حذف خودکار تاریخچه‌ها :**

"Delete browsing history on exit"را در تب "General" انتخاب کنید .

پاک کردن تاریخچه‌ی مرورهایتان پس از پایان هر جلسه، کمک میکند که اطلاعاتی که اینترنت اکسپلورر هنگام مرورهایتان ذخیره میکند، محدود شود .

❖ **ب) تنظیمات حریم خصوصی، privacy settingsرا انجام دهید :**

۴. **در تب privacy، این موارد را کامل کنید :**

Internet zone privacyرا بر روی "Medium High" یا higher قرار دهید .

این کار، مطمئنا تعدادی از کوکیها را مسدود میکند تا سایتها را از ردیابی شما یا تماس آنها با شما (بدون اجازه و رضایت شما بازدارد .

۵. **Location:**

"Never allow websites to request your physical location"را انتخاب کنید تا هرگز به سایتها برای درخواست مکان فیزیکی شما اجازه ندهد.

۶. **Pop-up Blocker:**

مطمئن شوید که Pop-up Blocker فعال باشد .

❖ پ) تنظیمات پیشرفته‌ی امنیت، **security** را انجام دهید :

به قسمت **"Security"** در تب **"Advanced"** رفته و این موارد را اعمال کنید :

۷. مطمئن شوید که تنظیمات به حالت پیشفرض خود مانده باشند .

اگر مطمئن نیستید، بر روی **"Restore advanced settings"** ، قبل از انجام هر تنظیم دیگری کلیک کنید (تا تنظیمات، به حالت اولیه و پیشفرض خود بازگردد .

۸. گزینه‌ی **"Do not save encrypted pages to disk"** را انتخاب کنید .

این کار، حافظه‌ی نهانگاهی از صفحات **https** را هنگامی که مرورگر بسته شود، حذف خواهد کرد .

منظور فایلهاییست که ممکن استدر حافظه‌ی پنهان سیستم مخفی شوند.

۹. تعیین کنید که :

"Empty Temporary Internet Files folder when browser is closed."

بدین معنی که پوشه فایلهای موقتی اینترنت، هنگامی که مرورگر بسته میشود، خالی شود .

این کار، اینترنت اکسپلورر را از ذخیره کردن اطلاعات شما شامل اطلاعات ورود به حسابهای کاربریتان، رمزهای عبور، فعالیتهایتان و ... فراتر از جلسه‌ی مرورتان بازمیدارد .

۱۰. تکمیل خودکار، **(auto complete)** را خاموش کنید :

ویژگی تکمیل خودکار، باید برای فرمها، نامهای کاربری و رمزهای عبور غیر فعال باشد .

غیر فعال نگه‌داشتن تکمیل خودکار، اطمینان میدهد که اطلاعات حساس شما، بدون ضرورت ذخیره نمیشود .

۱۱. حفاظت در برابر ردیابی : **(tracking protection)**

ویژگی حفاظت در برابر ردیابی در اینترنت اکسپلورر، مرورهای شما را از وبسایتهای تعیین شده شخص ثالث، **(third-party websites)**، مخفی نگه‌میدارد .

این ویژگی از طریق منوی **"Safety"** قابل دسترس است .

برای اینکه از قابلیت حفاظت در برابر ردیابی استفاده کنید،

نیاز دارید که فهرستی از حفاظتها در برابر ردیابی تهیه کنید

و در آن همه‌ی سایتهایی که نمیخواهید اطلاعاتتان برای آنها فرستاده شود، نام ببرید .

شما میتوانید فهرست را خودتان تهیه کنید یا آن را به صورت آنلاین دانلود کنید .

❖ **امنیت مرورگرها، عنصر مهمی در تأمین حفاظت از اطلاعات شماست :**

ویژگیهای مرورگرها و آسیبپذیریهای امنیتی آنها :

مرورگرهای شما پنجره‌ای به سوی اینترنت و نیز اولین ابزار برای دفاع از شما در برابر تهدیدات بدافزارهاست .

با رعایت نکاتی که قبلا مطرح شد و این نکاتی که در تنظیمات امنیتی مرورگرهایتان انجام میدهید، تا حدود زیادی امنیت خود را در اینترنت تضمین میکنید .

مرورگرها ابزارهای جانبی زیادی برای کارهای مختلف استفاده میکنند .

مانند Java, Flash Player, ActiveX, :و...

اما این ابزارها معمولا با نقصهای امنیتی همراه هستند .

که مجرمان سایبری، با سوء استفاده از این نقایص امنیتی، به سیستمهای شما دسترسی مییابند .

ActiveX را غیر فعال کنید :

یک افزونه برای مرورگر که به همراه مرورگرهای microsoft internet explorer و microsoft edgeآمده و فقط با این مرورگرها کار میکند .

با دادن راه نفوذ برای سایتهای خطرناک، به کامپیوترهای شما باعث مشکلات امنیتی میشود .

activexاین روزها به ندرت استفاده میشود، بنابراین مراقب باشید اگر سایتی از شما درخواست کرد که آن را نصب کنید، (فقط در صورتی با نصب آن موافقت کنید که ۱۵۰٪ مطمئن هستید آن سایت امن است .

در اینترنت اکسپلورر، همچنین در منوی tools, manage addon, تمامی افزونه‌ها را غیر فعال نمایید .

خصوصا اینکه مربوط به javascript, silverlight, activex, adobe flash, shockwaveو ... باشند .

برنامه‌های adobe, shockwave player, java, babylon و ... را بر روی سیستمهای خود نصب نکنید !

بویژه، javaوjavascript که باعث میشود هکرها بتوانند کنترل کامل سیستم مورد نظرشان را در اختیار خود داشته باشند !

غیر فعال کردن javascript, اگرچه در عملکرد برنامه‌هایی مثل google docs و youtube که برای کار کردن به آن نیاز دارد اختلال ایجاد میکند، اما به طور قابل ملاحظه‌ای تبلیغات، پاپآپها، و ... را غیر فعال میکند، زمان مورد نیاز برای بارگذاری صفحات وب را بسیار کاهش میدهد و بطور کلی، تجربه‌ی بهتری در استفاده از اینترنت برای شما فراهم میکند .

علیرغم چیزی که به نظر میرسد، این موضوع حادی نیست، چرا که مرورگرها این اجازه را به شما میدهند تا سایتهای معینی که میتوانند javascript را اجرا کنند، به لیست سفید اضافه کنید .

به دلیل اطلاعات مهمی که کوکیها دارا هستند، کوکیها اولین و اساسیترین هدف مجرمان سایبری هستند .

خصوصا آنهایی که ایمیلها، نامهای کاربری و رمزهای عبور را در بر دارد .

هنگامی که کوکیها را غیر فعال و حذف میکنید، اطلاعاتی که مجرمان سایبری میتوانند به دست بیاورند، بسیار کم میکنید .

کوکیها به دو دسته تقسیم میشوند :

کوکیهای اولیه و کوکیهای ثانویه .

1/کوکیهای نوع اول، (first-party) کوکیهایی هستند که وقتی از سایتی بازدید کنید، ممکن است بر روی سیستمتان ذخیره شود .

/2کوکیهای نوع دوم، (third-party)

کوکیهایی که از سایتهای دیگر در سیستمتان ذخیره میشوند .

کوکیهای نوع اول معمولا برای ذخیره‌ی اطلاعات ورود شما به کار گرفته میشوند تا مجبور نباشید هر بار که وارد سایتی میشوید، آنها را وارد کنید .

اما به مرورگرهایتان اجازه‌ی ذخیره‌ی رمزهای عبور را ندهید.

کوکیهای نوع دوم، تقریبا همیشه بوسیله‌ی تبلیغگران و بازاریابهای تجاری در کامپیوترتان قرار داده میشوند که علاقه‌مند به ردیابی کارهای آنلاین شما هستند. بنابراین، اگر آنها را مسدود کنید، اتفاق بدی نمی افتد.

وصله‌ها و افزونه‌های مرورگرها قابلیتهای جدیدی به آنها اضافه میکنند، ولی ریسک امنیتی را نیز به همراه دارند .

زیرا میتوانند دریچه‌ای به سیستمتان باز کنند که بتوان از آن برای وارد کردن بدافزارهابه سیستمتان سوء استفاده کرد .

در تنظیمات اینترنت اکسپلورر، در قسمت "Trusted sites" security شما میتوانید سایتهایی را که یقینا میدانید احتمال خطر ندارند،

بنابراین، میتوانید تنظیمات امنیتی پایینتری برای آنها قرار دهید تا تمام امکانات و ویژگیهای این سایتها برایتان فعال شود .

در محل"Restricted sites" ، میتوانید وبسایتهایی که میدانید خطرناک هستند را یادداشت کنید تا اینترنت اکسپلورر، بتواند در حالی که در این صفحات هستید، بیشترین تنظیمات امنیتی را برای آنها اعمال کند .

پیشنهاد این است که در قسمت (privacy) تمام کوکیهای نوع اول و دوم غیر فعال شوند،

مگر سایتهایی که مرتب از آنها بازدید میکنید، برای اینکه به درستی کار کنند، به این کوکیها نیاز داشته باشند .

اکنون، دکمه‌ی "Sites" را بفشارید و به این منو بروید .

در اینجا میتوانید بنویسید کدام وبسایتها اجازه ذخیره‌ی کوکیها را از طرف شما دارند و در کدامیک از کوکیها باید مسدود شود .

در لیست حرکت کنید تا گزینه‌ی "Enable third party browser extensions*" را پیدا کنید و آن را not check کنید .

انجام این کار، هر افزونه و وصله‌ی مرورگر که شما ممکن است داشته باشید را غیر فعال میکند .

که از نظر جنبه‌ی امنیتی راهکار خوبی است،

چون بسیاری از آنها در زمینه‌ی ردیابی مخفیانه‌ی رفتار کاربر، همچنین آسیبپذیریهای بالقوه‌ی امنیتی، و ... شناخته شده هستند .

- **چند نکته‌ی دیگر برای فایرفاکس :**

در تب "General" , در قسمت دانلود، تعیین کنید که همیشه درباره محل ذخیره‌ی فایلهایی که دانلود میکنید، از شما پرسش کند . "Always ask me where to save files" .

از این طریق، شما محل مشخصی برای فایلهای دانلود شده در وب ندارید که از این راه، تلاش شود بطور خودکار، محتواهای خطرناک بر روی کامپیوترتان ذخیره کند .

در این هنگام، این امکان به شما داده میشود تا محتواهای مشکوک را در محل امنی قرار دهید که بعدا بتوانید آنها را بررسی نمایید .

(در فایرفاکس ۴۹ به بعد)، در تب "manage your Do Not Track settings" , (privacy) را انتخاب و "Always apply do not track" را فعال کنید .

در حالی که در تب (privacy) هستید، در قسمت ,(history) گزینه‌ی "Firefox will never remember history" را انتخاب نمایید .

"Always use private browsing mode" دقیقا مساوی "never remember history" است. این گزینه زمانی اهمیت بیشتری دارد که بدانید دستگاهتان، ممکن است توسط افراد دیگر نیز استفاده شود .

برای اینکه بر تاریخچه‌ها کنترل بیشتری داشته باشید،

"Use custom settings for history" را انتخاب کنید .

با انتخاب گزینه‌ی ,"Always use private browsing mode" بنابراین، هرگاه شما مرورگر فایرفاکس را ببندید، تاریخچه‌ی مرورها، نتایج جستجوها، کوکیها و تاریخچه‌ی دانلودها را پاک میکند .

- **دو نکته‌ی امنیتی در گوگل کروم :**

در قسمت پلاگینها، شما میتوانید "Let me choose when to run plugin content" را انتخاب کنید. این موضوع، کنترل بیشتری نسبت به پلاگینها به شما میدهد و همچنین پلاگینهای آلوده را از نصب بدافزارها بر روی کامپیوترتان، بازمیدارد .

در قسمت دانلود، چک کنید تا همواره محل ذخیره کردن فایلها قبل از دانلود، از شما سؤال شود .

"Ask where to save each file before downloading".

انجام این کار، بسیاری از نرم‌افزارهای خطرناک را از دانلود خودکار بر روی کامپیوترتان بازمیدارد و همچنین، کنترل بهتری نسبت به آنچه که به کامپیوترتان وارد میشود، به شما میدهد .

نکات امنیتی درباره این سه مرورگر، بطور کامل در قسمتهای قبل شرح داده شد.

- **راهکارهای امنیتی برای microsoft edge**

برای microsoft edge نیز، "Settings" را انتخاب کنید .

دکمه‌ی "advanced settings" را پیدا کنید .

flash player یک هدف محبوب برای هک کردن کامپیوترها توسط مجرمان سایبری است .

به خاطر آسیبپذیریهای متعدد adobe-flash، چه خوب است که همگی آنها را غیر فعال کنید .

بعضی از صفحات و ویژگیهای سایتها ممکن است کار نکنند، (از طرف دیگر هرزنامه‌ها و عناصر مزاحم صفحات نیز، کار نمیکنند.

در بخش دانلود، مطمئن شوید که گزینه‌ی "Ask me what to do with each download" انتخاب باشد .

این امر، مرورگر را از دانلود خودکار بدافزارها یا هر نرم‌افزار بالقوه خطرناک دیگری بر روی کامپیوتر شما بازمیدارد .

در بخش privacy و security ، "Save form entries" and "Offer to save passwords" را غیر فعال کنید .

این موضوع از موارد مهم حیاتیست که هر راهی که برای مجرمان سایبری امکان دست‌درازی به حسابهای ارزشمند، رمزهای عبور و اطلاعات شخصی شما را فراهم میکند، ببندید .

فراموش نکنید تا گزینه‌ی "Send Do Not Track requests" را روشن کنید تا درخواست شما مبنی بر ردیابی نشدن، برای سایتها ارسال شود.
هنگامی که آن را روشن کنید، مرورگرتان به سایتها هشدار میدهد که نباید شما را در اینترنت ردیابی کنند .
بنابراین، در تنظیمات مرورگرهای خود، تکمیل خودکار رمزهای عبور و ذخیره‌ی آنها را غیر فعال کنید .
با انجام این تنظیمات، وقتی بخواهید وارد حساب کاربری خود در سایتها شوید، نیاز است هر بار نام کاربری و رمز عبور خود را وارد کنید .
با این وجود که هر بار نوشتن این اطلاعات دشواریهایی به همراه دارد، اما شما خطر دست‌درازی مجرمان سایبری را به چنین اطلاعات مهمی برای خود نمیخرید .

- **چند نکته‌ی مهم امنیتی دیگر :**

از حملات فیشینگ (سارقان اطلاعات)، دوری کنید .
در اینگونه حملات، مجرمان سایبری تلاش میکنند تا شما را با کلیک کردن بر روی لینکهایی آلوده که حاوی بدافزارها هستند، از طریق جعل هویت و وانمود کردن خود بعنوان افراد یا شرکتهای مورد اعتماد مانند بانک یا سرویس دهنده‌ی اینترنت، فریب دهند .
به محض اینکه بر روی لینک فیشینگ سارق اطلاعات کلیک کنید، بدافزار سیستم شما را آلوده میکند .
از رمز عبور یکسان برای تمام حسابهای کاربری خود استفاده نکنید .
در این صورت، مجرمان سایبری نمیتوانند یک رمز عبور را برای دستیابی به تمام حسابهای کاربری آنلاین شما بارها استفاده کنند .
بررسی کنید که سایت به جای (http, (https باشد .
سایتهایی که از https استفاده میکنند، یک لایه‌ی امنیتی بیشتر به وبسایت خود می‌افزایند .
s به معنی) secure امن) است،
بدین معنی که اطلاعات بین مرورگر شما و وبسایت مورد نظرتان رمزگذاری میشوند و این امر، کار را برای هکرها بسیار دشوار میکند که به اطلاعاتتان دست بیابند .
ایمیل کاری خود را از ایمیلی که برای حسابهای کاربریتان استفاده میکنید، مجزا کنید .
وقتی به شبکه‌های بیسیم عمومی و یا رایگان متصل میشوید، دقت کنید .
یکی از روشهای مورد علاقه‌ی مجرمان اینترنتی که از آن برای به دست آوردن مدارک و اطلاعات شما استفاده میکنند، همین شبکه‌های بیسیم و اطلاعاتی است که رد و بدل میشود .

❖ **جلوگیری از ردیابی کاربر در اینترنت (tracking) :**

وبسایتها میتوانند رفتار و مرورهای کاربران خود را ردیابی کرده و این اطلاعات را در اختیار افراد و شرکتهای دیگر قرار دهند یا بفروشند .

ویژگی (tracking protection) در فایرفاکس، در نسخه‌های قدیمیتر، فقط در مرور عادی (regular browsing) وجود داشت،

اما از نسخه‌ی ۴۲ این قابلیت در مرور ناشناس , (private browsing) بطور پیشفرض فعال است .

البته در مرور عادی این گزینه یعنی محافظت در برابر ردیابیها بطور پیشفرض فعال نیست، و شما باید با استفاده از تنظیمات، آن را فعال کنید .

در فایرفاکس ۴۹ به بعد :

در تنظیمات (privacy) , manage your Do Not Track settings را انتخاب و گزینه‌ی Always apply Do Not Track را فعال نموده و بر روی دکمه‌ی okay کلیک کنید تا این تنظیم اعمال شود .

در فایرفاکس ۴۲ تا قبل از ۴۹ :

در تنظیمات (privacy) , request that sites not track you را فعال کنید .

در ورژنهای قبل :

در تنظیمات (privacy) , tell sites that i do not want to be tracked را فعال نمایید .

در فایرفاکس ۴۲ در تنظیمات , (privacy) فقط میتوانید تعیین کنید که محافظت در برابر ردیابیها در مرور ناشناس فعال باشد یا نه، و امکان انتخاب موارد را ندارید .

اما از نسخه‌ی ۴۳ به بعد، امکان بهره‌مندی از (disconnect me) به مرورگر اضافه شده است که با انتخاب گزینه‌ی Change Block List در تب , (privacy) به آن دست مییابید .

Disconnect.me basic protection (Recommended). Allows some trackers so websites function properly.

(حفاظت مقدماتی است که به بعضی از ردیابها اجازه‌ی فعالیت میدهد تا سایتها به درستی کار کنند .)

Disconnect.me strict protection. Blocks known trackers. Some sites may not function properly.

) حفاظت دقیق و کامل است که همه‌ی ردیابهای شناخته شده را مسدود میکند، اما ممکن است بعضی از سایتها به درستی کار نکنند . (

تجربه‌ی خودم: این گزینه را بر روی strict protection تنظیم کردم و مشکلی نداشتم .

چند قابلیت و امکان جدید در برخی نسخه‌های فایرفاکس :

محافظت در برابر بدافزارها و نرم‌افزارهای خطرناک، از نسخه‌ی ۳۱ به فایرفاکس اضافه شده است .

در نسخه‌ی ۴۰، مسدود کردن فایلهای خطرناک هنگام دانلود افزوده شده و

در نسخه‌ی ۴۸، با اضافه شدن گزینه‌ی هشدار درباره دانلود نرم‌افزارهای ناخواسته و نامتعارف کاملتر شده است .

در نسخه‌ی ۴۳، محافظت در برابر سارقان و بدافزارها همچنان فعال است، اما به دلیل یک باگ که در نسخه‌های بعدی اصلاح شده، محافظت در برابر فایلهای مخرب که دانلود میشود، وجود ندارد .
از نسخه‌ی ۴۴، گزینه‌ای به نام push notification به فایرفاکس اضافه شده است .
برای غیر فعال کردن آن، در منوی options , در تب content , با کلیک بر روی گزینه‌ی choose , (remove all sites) را انتخاب کنید و تغییرات را ذخیره نمایید .
ضمنا در نسخه‌ی ۴۹، به روز رسانی مدیریت ورود به حساب کاربری، انجام شده است .
که اجازه میدهد صفحات https , از اطلاعات ورود ذخیره شده در http نیز استفاده کنند .
این کار، روشی برای رمزگذاری بهتر فایلها و تحول به سوی اینترنت امنتر است .
در فایرفاکس ۵۰ نیز، محافظت از کاربر در برابر تعداد قابل توجهی از فایلهای اجرایی برای سیستم عاملهای ویندوز، لینوکس و مک به مرورگر افزوده شده است .
در ویندوز، برای استفاده از فایرفاکس ۴۹ به بعد، در صورتی که پردازنده‌ی کامپیوترتان از sse2 پشتیبانی نمیکند، آن را ارتقا دهید .

- برای دستیابی به تنظیمات پیشرفته‌ی فایرفاکس :

در نوار آدرس about:Config را تایپ کرده و اینتر نمایید .
پیامی برایتان ظاهر میشود که به شما هشدار میدهد، در صورتی که این تنظیمات پیشرفته را تغییر دهید، ممکن است برای پایداری، امنیت و اجرای نرم‌افزار زیانبار باشد .
فقط در صورتی ادامه دهید که از کاری که میخواهید انجام دهید، مطمئن باشید .
بر روی دکمه‌ی I'll be careful, I promise! کلیک کنید .
تنظیمات موجود را میتوانید با استفاده از کلید enter و یا راست کلیک و انتخاب گزینه‌ی Toggle تغییر دهید .
توجه: همانطوری که هشداری که به آن اشاره کردم بیان میکند، تغییر دادن این گزینه‌ها بدون اطلاع از عملکرد و نتیجه‌ی آنها، ممکن است خطرناک باشد و بنابراین قبل از تغییر گزینه‌ها از درستی کار خود مطمئن شوید .
توجه: اکثر این گزینه‌ها به حالت پیشفرض، مطلوب است و اصلا نباید تغییر داده شود !
در کادر جستجو این گزینه‌ها را وارد کرده و در صورتی که با الگویی که مینویسم مطابق نبود، آنها را تغییر دهید .
دقت کنید که گزینه‌هایی که مینویسم دقیقا تنظیماتش را مطابق این الگو انجام دهید :

```
privacy.trackingprotection.pbmode.enabled default boolean true
```

برای فعال بودن گزینه‌ی حفاظت در برابر ردیابی در حالت مرور ناشناس.

```
extensions.blocklist.enabled true
```

برای اینکه افزونه‌های خطرناک را مسدود کند.
از نسخه‌ی ۴۸ به بعد، افزونه‌های غیر رسمی که توسط شرکت موزیلا تأیید نشده باشند، اجرا نمیشوند .

```
dom.push.enabled false
```

برای غیر فعال کردن امکان push notification که به نسخه‌ی ۴۴ به بعد، اضافه شده است.
به دلیل اینکه notification ها حتی بعد از بستن صفحه‌ی مورد نظر نیز برای شما ارسال میشوند، و نیز، به این دلیل که سایتها آیپی سیستم شما را برای فرستادن اطلاعات در اختیار دارند، حتما این امکان را غیر فعال نمایید .
البته سایتها برای فرستادن اطلاعات به تأیید شما نیاز دارند.

این اطلاعات شامل تبلیغات تجاری، پیامهای سایت، مطالب جدید سایت و ... میشود .
بنابراین، با انجام مواردی که در این زمینه نام بردم، دریافت push notification برای شما در فایرفاکس غیر فعال میشود .
با غیر فعال شدن این امکان، شما دیگر توسط سایتهایی که این امکان را پشتیبانی میکنند، یادآوری برای ارسال اینگونه پیامها را به سیستمتان دریافت نمیکنید .

```
plugins.click_to_play true
```

این امکان را میدهد که پلاگینها، تنها با اجازه و تأیید کاربر اجرا شوند.
با فعال بودن گزینه‌یClick to Play ، آن دسته از محتواهای وب که به پلاگین نیاز دارند، پلاگینهایی مانند : Java, Flash, Silverlight, Adobe Reader, QuickTimeو ... بصورت پیشفرض غیر فعال میشوند .
کاربران باید بصورت دستی بر روی آن دسته از محتواها که به پلاگین نیاز دارند، کلیک کنند تا بتوانند آن محتواها را در صفحه‌ی وب مورد نظر دریافت کنند .
این کار، کنترل امنیتی مؤثری برای کاربر ایجاد میکند، بنابراین، محتواهای خطرناک بطور خودکار در مرورگر اجرا نمیشوند .

```
javascript.enabled false
```

برای غیر فعال کردن اسکریپتهای جاوا که کنترل سیستم را از راه دور بطور کامل برای هکرها فراهم میکند .

```
browser.urlbar.autocomplete.enabled false
```

برای غیر فعال کردن تکمیل خودکار در نوار آدرس مرورگر.

```
browser.search.suggest.enabled false
```

برای غیر فعال کردن پیشنهادهای جستجو توسط موتورهای جستجوگر.

```
extensions.pocket.enabled false
```

غیر فعال کردن امکان ذخیره‌ی اطلاعات درpocket
در صورتی که از فایرفاکس ۴۸ و قبلتر استفاده میکنید،

```
loop.enabled false
privacy.trackingprotection.enabled true
privacy.donottrackheader.enabled true
```

هر دو برای حفظ حریم خصوصی و جلوگیری از ردیابی رفتارهای کاربر در اینترنت.
در صورتی که در تنظیمات privacy, گزینه‌ی always apply do not track را مشاهده نکردید، این گزینه را که به صورت پیشفرض false است، trueنمایید .

```
privacy.trackingprotection.ui.enabled
```

سپس در تنظیمات privacy, do not track را بر روی always تنظیم کنید .

```
plugin.scan.plid.all false
```

این گزینه نیز حتما falseباشد تا پلاگینهای موجود در سیستم، توسط مرورگر اسکن نشده و بطور خودکار به مرورگر اضافه نشود.
این موضوع نیز، برای حفظ امنیت کاربر مؤثر است.

```
media.autoplay.enabled false
```

راهکار جلوگیری از پخش خودکار فایلهای صوتی-تصویری در فایرفاکس ۲۶ به بعد.

برای جلوگیری از پخش خودکار ویدیوهای html5 .

از نسخه‌ی ۲۶ به بعد، در صورت دانلود فایلهای چندرسانه‌ای با فایرفاکس، فایلهای صوتی تصویری به جای نمایش پنجره‌ی دانلود که بتوانید دریافت یا باز شدن فایل را انتخاب کنید،
فایلها بطور خودکار پخش میشوند و نمیتوانید آنها را دانلود کنید !
برای غیر فعال کردن این امکان، و دسترسی به امکان انتخاب دانلود و یا پخش فایل، گزینه‌ی
media.directshow.enabled false باشد .
در ویندوزهای جدیدتر از xp , این گزینه‌ها را نیز false کرده و امتحان نمایید .

```
media.windows-media-foundation.enabled
media.play-stand-alone
```

- دانلود فایلها با خود مرورگر firefox ، بدون نیاز به برنامه‌های مدیریت دانلود ! :

در فایرفاکس نسخه‌ی ۳۳ به بعد، میتوانید فایلهای خود را بدون نیاز به برنامه‌های مدیریت دانلود، به راحتی با خود مرورگر دانلود نمایید .
در نسخه‌های قبل، در صورتی که اتصال شبکه یک لحظه قطع میشد، فایل دانلود شده متوقف و امکان ادامه‌ی دانلود را نداشتید .
در این صورت، باید دانلود فایل را مجددا از ابتدا شروع میکردید .
اما این مشکل در نسخه‌ی ۳۳ شروع به اصلاح و در نسخه‌ی ۳۹ به بعد، بطور کامل برطرف شده است .
بدین معنی که در صورت قطع شبکه و اتصال مجدد آن، امکان ادامه‌ی دانلود، دکمه‌ی (resume , retry) یا برای ادامه‌ی دانلود فایلهای ناقص دانلود شده، از همانجایی که دانلود متوقف شده، در اختیارتان قرار دارد .

- control center و اطمینان از امنیت سایتهایی که بازدید میکنیم :

قابلیت (control center ,) از نسخه‌ی ۴۲ به بعد به مرورگر فایرفاکس اضافه شده است .
با کلیک بر روی این گزینه و انتخاب site info و نیز، more information , شما میتوانید درباره سایتهایی که میخواهید از آنها بازدید کنید، فایل دانلود کنید و یا حساب کاربری ایجاد نمایید، از نظر حفظ امنیت و حریم خصوصیتان و موارد متعدد دیگر اطلاعات به دست آورید .

درباره پلاگینها در گوگل کروم و فایرفاکس :

addons را از منوی tools فعال کنید .
به بخش پلاگینها سویچ کنید .
در این قسمت، لیستی از پلاگینهای نصب شده را میبینید .
هر کدام از پلاگینها میتواند به یکی از سه حالت زیر، تنظیم شود :

Never activate means it is disabled. (غیر فعال)
Always activate means it is enabled. (فعال)
Ask to activate enables click to play. (پرسش از کاربر برای فعال شدن)

در نوار آدرس، میتوانید about:plugins را تایپ کرده و اینتر نمایید .
این صفحه، برای شما جزئیات بیشتری درباره پلاگینهای نصب شده به همراه فایرفاکس ارائه میدهد .
اگرچه از این طریق، نمیتوانید پلاگینی را فعال یا غیر فعال کنید، اما مسیر دقیق نصب پلاگین و نیز، فایلهایی که به همراه آنها استفاده شده است، نمایش میدهد .
این گزینه برای اینکه بدانید چرا و از کجا این پلاگینها ناگهان وارد فایرفاکس شده است، بسیار مؤثر است .
حالت همیشگی :
شما میتوانید حالت همیشگی را برای فایرفاکس تعیین کنید، اگر نمیخواهید پلاگینها هیچوقت در مرورگر فعال باشند، این کار بسیار مفید است .
ابتدا مطمئن شوید که به روز رسانی گوگل، در فایرفاکس فعال نباشد .
1/در نوار آدرس مرورگر about:Config را تایپ کرده و کلید اینتر را بفشارید .
2/بعد از ظاهر شدن پیام هشدار، بر روی دکمه‌ی I'll be careful, I promise! کلیک کنید .
3/با استفاده از کادر جستجو plugin.state را بیابید تا لیست پلاگینهای نصب شده، برایتان نمایش داده شود .
آنها به همراه اعداد ۰، ۱، ۲ هستند یا عددی به همراه خود ندارند .
۰ (غیرفعال)، ۱ (click to play) فعال است و برای اجرا، از کاربر تأیید میخواهد. ۲ (فعال).
بدون عدد نیز بدین معنیست که هنوز برای آن، تنظیمی اعمال نشده است .
برای اینکه اجرای پلاگینها را یکجا غیر فعال کنید،

plugin.default.state default integer 1

اگر برای شما نیز، عدد یک یا هر عدد دیگری بود، آن را پاک کرده و به جای آن، ۰ تایپ کنید .
پیشنهاد میکنم برای جاوا و ادوبی، حتما جداگانه عدد را برای احتیاط بیشتر، صفر قرار دهید .
و همانطور که قبلا مطرح شد، برای اینکه پلاگینها اسکن نشده و به مرورگر افزوده نشوند،
plugin.scan.plid.all user set boolean false باشد .
برای فعال کردن گزینه‌ی click to play در پلاگینها در گوگل کروم :
به تنظیمات بروید، بر روی "Show advanced settings" کلیک کنید .
در تنظیمات privacy، بر روی تنظیمات محتوا "Content settings" و در قسمت پلاگینها، گزینه را به نحوی تغییر دهید که برای اجرای پلاگینها، نیاز به تأیید شما باشد .
یعنی "Click to play"

- **منبع توضیحات درباره پلاگینهای فایرفاکس :**

اجرای پلاگینهای npapi, از نسخه‌ی ۴۷ به بعد، بدون تأیید کاربر غیر فعال شده است و به خاطر مشکلات در اجرای مرورگر، crashو هنگ در برنامه و نیز، آسیبپذیریهای امنیتی که در آنها مشاهده شده است، از نسخه‌ی ۵۳ و ۵۲ ESR، بطور کامل حذف میشود .

- **نکات امنیتی عمومی و نکات مهم دیگر درباره فایرفاکس :**

برای جلوگیری از حملات هکرها و باج‌افزارها، ایمیلهای اسپم را باز نکنید، به آنها پاسخ ندهید، بر روی لینکهایی که میفرستند، کلیک نکنید، فایلهای ضمیمه‌ی آنها را دانلود نکنید و اطلاعات شخصی خود را مانند حسابهای بانکی و رمزهای عبور، در اختیارشان قرار ندهید !
از سایتهای غیر اخلاقی و مشکوک، بازدید نکنید .
برنامه‌ی آفیس را طوری تنظیم نمایید که اجرای ماکروها در آن، به حالت high و یا بهتر است very high تنظیم شود .
اسناد آفیس را از افراد و سایتهای مطمئن دریافت نمایید .
از یک برنامه‌ی فایروال مطمئن و رایگان، مثل zonealarm free firewall, که در این زمینه یکی از بهترین انتخابهای شماست، استفاده کنید .
برای حفظ حریم خصوصی و اطلاعات ارزشمند خود، سعی کنید تا جایی که میتوانید، از فیلتر شکن استفاده نکنید !
بهترین راه در امان ماندن از خطرات باج‌افزارها، این است که بطور مرتب از تمامی داده‌های ارزشمند خود، نسخه‌ی پشتیبان تهیه کرده، آنها را در cd وdvd های با کیفیت رایت نموده و در مکانهای امن، نگهداری کنید تا در صورت بروز خطر، به راحتی بازیابی نمایید .
فایلهای ناشناخته‌ی اجرایی که به آنها اطمینان ندارید، با پسوندهای msi, exe, vba, vbs, vb, com, batها و ... را بهیچ عنوان اجرا نکنید ! shortcut,
هنگام نصب برنامه‌ها، ابتدا سعی کنید اتصال اینترنت خود را قطع کنید، سپس نرم‌افزار را بصورت custom) یا advanced install)نصب کنید .
تمامی برنامه‌ها و تولبارهای ناخواسته که به همراه نرم‌افزار ممکن است نصب شوند، غیر فعال کنید !
توجه: تمامی برنامه‌ها دارای تولبارهای اضافی و موارد مخرب نیستند، و برای اینکه مطمئن شوید چه چیزی نصب میکنید، از نصب (typical) یا خودکار، پرهیز کنید .
قبل از نصب برنامه‌ها، حتما موافقتنامه‌ی آنها را مطالعه نمایید تا بدانید در صورت استفاده از برنامه، چه اتفاقی ممکن است پیش بیاید !
در مواردی میتوان، با خواندن توافقنامه، به امنیت و یا عدم برنامه‌ها تا حدود زیادی پی برد !
در شبکه‌های اجتماعی نیز، فایلها و لینکهای مشکوک که به آنها اطمینان ندارید، باز نکنید !
نرم‌افزارهای کرک شده و غیر قانونی تا حد ممکن استفاده نکنید !
اینگونه نرم‌افزارها علاوه بر اینکه از نظر شرعی، عرف و اخلاق جایز نیستند، فایلهای patch و keygen در موارد زیادی ممکن است ماهیت خطرناک داشته باشند و اطلاعات محرمانه‌ی شما را از طریق کرک (crack) کردن برنامه‌ها برای هکرها ارسال کنند !
اکثر برنامه‌های پولی که کرک میشوند، جایگزینهای مشابه رایگان و حتی در مواردی بهتر از همتای پولی خود دارند .

پس از آنها استفاده کنید .
نرم‌افزارها را حتما از سایتهای معتبر دریافت نمایید .
خصوصا برنامه‌های متنباز (opensource) که کدهای برنامه‌نویسی آنها در اختیار عموم قرار دارد، از سایتهای معتبر و بویژه سایت سازنده دریافت نمایید .
دریافت برنامه‌ی متنباز از سایت سازنده، علاوه بر امنیت و اطمینان بیشتر، باعث تشویق و کمک به توسعه دهندگان اینگونه نرم‌افزارها نیز میشود و برای همین، بسیار اهمیت دارد .
آخرین نسخه‌ی فایرفاکس را از

https://www.mozilla.org/firefox/

دریافت نموده و برای دستیابی به نسخه‌های قبل و انتخاب نسخه‌ی مورد نظر خود، از این لینک استفاده کنید .
توجه: نسخه‌های خیلی قدیمی و همچنین نسخه‌های آزمایشی را که حرف b دارند، به دلیل امکان داشتن باگهای امنیتی دانلود نکنید !
معمولا در اکثر موارد آخرین نسخه، بهترین نسخه هم هست .

https://ftp.mozilla.org/pub/mozilla.org/mozilla.org/firefox/releases/

هنگام نصب فایرفاکس، آن را به روش (custom setting) , نصب کنید و (maintenance service)را بدون علامت نمایید تا نصب نشود .
این گزینه امکان به روز رسانی نرم‌افزار را بدون دخالت کاربر بطور خودکار، فراهم میکند .
اما در مواردی مشکلات امنیتی در آن وجود داشته که توسط شرکت سازنده، در حال برطرف شدن است .
بنابراین، آن را غیر فعال کنید و فایرفاکس خود را بطور دستی آپدیت نمایید .
فایرفاکس، معمولا هر ۶هفته یک بار، نسخه‌ی پایدار و رسمی ارائه میدهد که بهتر است برای امنیت بیشتر، آنها را دریافت نمایید .
تغییرات ورژنهای مختلف، اشکالات و همچنین باگهای امنیتی برطرف شده، امکانات جدید، تغییرات برای توسعه دهندگان را میتوانید از لینک اصلی سایت سازنده بخوانید .

https://www.mozilla.org/firefox/releases

در صورتی که واقعا به افزونه‌ای در مرورگر خود نیاز دارید آن را نصب کنید، وگرنه از نصب افزونه‌ها خودداری نمایید .
افزونه‌ها را نیز فقط از منبع اصلی آن دریافت نمایید .

https://addons.mozilla.org/en-US/firefox/

مژده به طرفداران و کاربران فایرفاکس که نمیخواهند از مرورگرهای دیگر استفاده کنند !

گزینه‌ی container به نسخه‌های جدید فایرفاکس اضافه شده است و در نسخه‌ی ۵۰ فایرفاکس بسیاری از باگهای آن برطرف شده و با اعمال تنظیماتی که در ادامه مطرح میشود، قابل استفاده میباشد !

Contextual Identities on the Web:

ویژگی containers در فایرفاکس به کاربران کمک میکند تا بتوانند در یک سایت، همزمان وارد چند حساب کاربری شوند .

و به کاربران این توانایی را میدهد که اطلاعات سایت را در حسابهای کاربری مختلفشان برای بهبود حریم شخصی و امنیت خویش از یکدیگر جداسازی کنند .

با containers, کاربران میتوانند چند تب را در چند بستر مختلف باز کنند،

Personal, Work, Banking, -و Shopping.

بدین معنی که اطلاعاتی که سایت از کاربران در یک بستر به دست میآورد، با اطلاعاتی که از کاربران در بستر دیگر به دست میآورد، تفاوت دارد .

شما میتوانید چند تب را در یک container مشخص در یک زمان باز کنید،

همچنین میتوانید چند تب را در چند container مختلف در یک زمان باز کنید .

شرایط مرور عادی شما container) پیشفرض)، به حالت عادی خود مانده و در تبهای معمولی شما باقی میماند .

ویژگی container, تجربه‌ی آشنا و عادی از مرور وب را که داشتید، در حال استفاده‌ی تب یا پنجره‌ی جدید تغییر نمیدهد .

تب معمولی همچنان به دسترسی اطلاعاتی از مرورگر که در گذشته ذخیره شده است ادامه میدهد .

محیط کاربری تب معمولی هنگام استفاده از تبهای container تغییر نمیکند .

هنگامی که از ویژگی container استفاده میکنید،

تبهای مختلف در آن، به اطلاعات سایت که در شرایط معمولی استفاده میکنید، دسترسی ندارد .

و همچنین هنگامی که از تبهای معمولی استفاده میکنید،

آن تب به اطلاعاتی از سایت که در تبcontainer های مختلف ذخیره شده است، دسترسی ندارد .

بطور معمول، هر نوع اطلاعاتی که سایتها امکان دسترسی به خواندن و نوشتن آن را دارند، باید از یکدیگر جدا شود .

تنها اطلاعاتی که سایت بدان دسترسی دارد جدا میشود، نه اطلاعاتی که کاربر بدان دسترسی دارد !

البته IP سیستم شما، نوع سیستم عاملتان و ... که برای همه تبها یکسان است، تغییر نمیکند و ممکن است ردیابی شود .

با استفاده از این قابلیت، که در منوی files قرار دارد، نیاز به استفاده از دو مرورگر بطور همزمان و همچنین خروج از یک حساب کاربری به منظور ورود به حساب جدید را ندارید .

بنابراین، دقت کنید که برای انجام کارهای مختلف ازcontainer های مختلف استفاده کنید .

مثلا برای حساب کاربری شخصیتان ,personal

برای اکانتها و امور کاریتان ,work

برای انجام امور مالی و بانکیتان banking و ... را استفاده کنید .

نحوه فعالسازی قابلیت container در فایرفاکس ۵۰ به بعد :

در نوار آدرس about:Config را تایپ کرده و پیامی که ظاهر میشود، accept کنید .

در قسمت جستجوی آن، این گزینه‌ها را تایپ کرده و در صورتی که false بود، با کلید enter آنها را true نمایید تا فعال شود .

1- privacy.userContext.enabled

گزینه‌ی اصلی برای فعال یا غیر فعال کردن قابلیت containers است .

2- privacy.userContext.ui.enabled

این گزینه نمایش یا عدم نمایش تنظیم فعالسازی containers را در options-privacy که در منوی toolsقرار دارد، تعیین میکند .
در صورت فعال بودن، گزینه‌ی Enable Container Tabs به تنظیمات privacy اضافه میشود .
3-میتوانید در فایرفاکس ۵۱ به بعد، گزینه‌ی
privacy.usercontext.about_newtab_segregation.enabled که مربوط به باز کردن تب جدید میشود را نیز فعال کنید، تا اطلاعات سایتها در تبهای مختلف از یکدیگر جدا شوند .
بنابراین، بهترین ورژن فایرفاکس که از این قابلیت بطور کامل پشتیبانی میکند، نسخه‌ی ۵۱ است .

- چند ویژگی مهم فایرفاکس ۵۱ و ۵۲ :

فایرفاکس ۵۱ :

1-پشتیبانی کامل از قابلیت containers چنانکه گذشت .
2-هشدار به کاربران در صورتی که اطلاعات کاربریشان را در سایتهای http یا بطور کلی فاقد امنیت وارد کنند که به صورت پیشفرض فعال است و در برخی نسخه‌های قبلی نیز میتوان با فعال کردن گزینه‌ی
security.insecure_password.ui.enabled
در تنظیماتabout:config
آن را فعال کرد .
این هشدار که با رنگ به کاربران نمایش داده میشود، بدین معناست که اگر رمزهای عبورتان را در این وبسایت که اتصال امنی ندارد وارد کنید،
ممکن است توسط هکرها و مهاجمان اینترنتی دزدیده شود .
در اینگونه موارد، اگر به امن بودن سایت مورد نظرتان اطمینان دارید،
سعی کنید ببینید آیا ورژن امن آن وجود دارد که از آن استفاده کنید،
بدین معنی که در ابتدای آدرس، https://وارد نمایید .
یا با مدیر سایت تماس گرفته و از آنها بخواهید اتصالهایشان را امن کنند .
موردی که پیشنهاد نمیشود !
شما میتوانید با وجود ناامن بودن اتصال، وارد آن شوید .
اما این کار را فقط با مسئولیت خودتان انجام دهید !
در این موارد، از یک رمز عبور یکتا یا رمز عبوری که از آن برای ورود به سایتهای مهم بهره نمیبرید، استفاده کنید .
3-بلاک برخی اسکریپتهای مخرب از لود و یا اجرا شدن که بطور پیشفرض فعال است .
فایرفاکس ۵۲ :

1-بهبود تجربه‌ی کاربران در دانلود .
2-فعال شدن touch برای کاربرانی که از تبلتها یا لپتاپهای لمسی استفاده میکنند .
3/هشدار متنی به کاربران در صورت ناامن بودن اتصال به یک سایت مشخص که بطور پیشفرض فعال است .
این هشدار، در نوار آدرس و پایین فیلد پسوردی که فکوس سیستم بر روی آن قرار دارد، در هر فرمی که ناامن باشد، نمایش داده میشود .

بعلاوه، پر شدن خودکار داده‌ها در سایتهای http و همچنین سایتهای ناامن در این نسخه بطور پیشفرض غیر فعال است .

همچنین هشدار درباره عدم امنیت فرمی که در آن اطلاعاتتان را وارد میکنید،

در نسخه‌های مختلف فایرفاکس، در جایگاه security در developer console نیز قرار دارد .

هکرها ممکن است از راههای مختلف مانند keylogger یا تغییر مسیر سایتی که کاربر اطلاعات شخصیش را بدان وارد میکند به سایت مورد کنترل خود،

به اطلاعات او دسترسی پیدا کنند .

تب security در Web Console به توسعه دهندگان و همچنین کاربران درباره مسائل امنیتی هشدار میدهد .

4- قرار دادن قانون کامل و دقیق برای امنیت کوکیها :

این کار، سایتهای http را از قرار دادن مشخصات کوکیهای امن برای فریب کاربران باز میدارد .

یعنی فقط کوکیهای امن میتوانند در سیستم ذخیره شوند !

منابع مربوط به امنیت صفحات دارای فرم فیلد غیر امن :

https://support.mozilla.org/en-US/kb/insecure-password-warning-firefox

https://developer.mozilla.org/docs/Web/Security/Insecure_passwords

چند نکته دیگر درباره فایرفاکس ۵۲ :

فایرفاکس ۵۲ در نسخه@ی معمولی، دیگر از ویندوزهای xp و vista پشتیبانی نمیکند !

آنها باید نسخه‌ی ESR فایرفاکس (extended supported release) را نصب کنند تا بتوانند از نسخه‌ی ۵۲ استفاده کنند،

و همچنین آپدیتهای امنیتی نیز تا چند ماه برای این کاربران ارائه میشود .

برای نمونه: لینک دانلود فایرفاکس ESR 32 بیتی (که البته بر روی هر دو نسخه‌ی ۳۲ و ۶۴ بیت از ویندوز اجرا میشود) در اینجا قرار میدهم .

https://ftp.mozilla.org/pub/firefox/releases/52.0esr/win32/en-US/Firefox%20Setup%2052.0esr.exe

در ورژن ۵۳ نیز، حداقل سیستم عامل مورد نیاز برای نصب فایرفاکس، ویندوز هفت میباشد .

اگر از کاربران windows xp هستید، حتما بخاطر مصونیت از باگهای نسخه‌های قدیمیتر، آن را به servicepack3 ارتقا دهید !

چنانچه گذشت، فایرفاکس ۵۲(نسخه‌ی معمولی) بطور پیشفرض، پلاگینهای netscape (npapi plugins) را جز flash, لود نمیکند .

اما کاربران نسخه‌ی ESR, باید این قابلیت را در تنظیمات about:config خود فعال کنند .

plugin.load_flash_only را در صورتی که از کاربران نسخه‌ی ESR هستید، true نمایید .

بهترین نسخه‌ی فایرفاکس از نظر من نسخه ۵۲ هست .

علاوه بر تمام مطالب مهمی که در این مقاله ذکر شد، (خصوصا قابلیتهای مهم جدید امنیتی)، از تمامی ویندوزها از xp گرفته تا ویندوز ده پشتیبانی میکند !

لینک دانلود نسخه‌ی معمولی فایرفاکس ۵۲:

https://ftp.mozilla.org/pub/firefox/releases/52.0/win32/en-US/Firefox%20Setup%2052.0.exe

❖ جایگزینهای رایگان چند برنامه‌ی پولی پر کاربرد :

۱. libreoffice به جای microsoft office

که بهترین برنامه در این زمینه میباشد .

در صورتی که به جای برنامه‌ی آفیس، فقط به word نیاز دارید، جایگزین متنباز و رایگان آن را از http://www.abisource.com/downloads/abiword/2.9.4/Windows/abiword-setup-2.9.4.exe دریافت نمایید .

این برنامه با حجم ۹مگابایت، قابلیتهای فراوان و سازگاری با اسناد microsoft word, بسیاری از نیازهای شما را در این زمینه تأمین میکند !

۲. sumatra به جای adobe reader

۳. gimp به جای photoshop

۴. inkscape به جای corel draw

۵. 7zip به جای winrar

۶. برای دانلود فایلها نیز، بهتر از خود فایرفاکس استفاده کنید یا به جای استفاده از internet download manager, آن را از نماینده‌ی رسمی آن، خریداری کرده یا از برنامه جایگزین رایگان آن، استفاده کنید .

۷. audacity برای ضبط، ویرایش و میکس فایلهای صوتی .

۸. دیکشنری رایگان ایرانی که میتواند بسیاری از نیازهای شما را برای یافتن ترجمه‌ی کلمات انگلیسی تأمین کند .

۹. تقویم ایرانی با قابلیتهای فراوان ازجمله : مبدل، نمایش مناسبتهای روز، اذکار و دعاهای روزانه، پخش اذان و اوقات شرعی شهرها، احادیثی از چهارده معصوم با ذکر منبع و . . .