

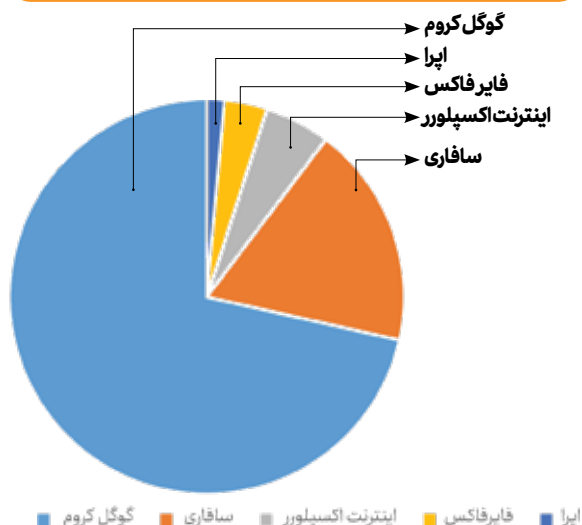


است. تمامی قابلیت‌های حالت استاندارد را دارد، اما به‌خاطر امنیت بیشتر، شاید عملکرد بعضی از سایت‌ها را مختل کند. همچنین در این حالت، ایجاد اثر انگشت از رفتار کاربر و همچنین ردیاب‌ها در تمامی تب‌ها، مسدود می‌شوند. حالت Custom یا سفارشی هم حالتی است که عموماً برای کاربران حرفه‌ای پیشنهاد می‌شود تا گزینه‌های بیشتری را برای تنظیمات حفاظت از حریم خصوصی در سایت‌های مختلف بررسی کنند.

سافاری

مرورگر سافاری که ساخته شرکت اپل است همیشه تمرکز زیادی روی حفاظت از حریم خصوصی داشته است. شرکت اپل قابلیت‌هایی به نام Intelligent Tracking Prevention در مرورگر اختصاصی عرضه کرده است. طبق آنچه خبرگزاری CNET گفته است؛ شرکت اپل قصد دارد در نسخه بعدی مرورگر سافاری، تنظیمات حفاظت در برابر ردیاب‌های وب را ارتقا دهد. این نسخه جدید قابلیت‌های مختلفی برای مقابله با ردیاب‌های اینترنتی دارد. به عنوان مثال این مرورگر به شما می‌گوید چه ردیاب‌هایی در وب‌سایتی که در حال مشاهده هستید، فعال هستند. همچنین کاربران می‌توانند یک گزارش ۳۰ روزه از ردگیری‌های انجام شده در وب‌سایت‌ها دریافت کنند. با وجود این برای اطمینان از این‌که این ردیاب‌ها در سافاری مسدود هستند، وارد بخش Preferences شوید و گزینه Privacy را لمس کنید. سپس گزینه Prevent cross-site tracking را فعال کنید تا وب‌سایت‌ها تاریخچه شما را از وب‌سایت‌های قبلی و بعدی، ردگیری نکنند. در همان بخش هم می‌توان کوکی‌های ذخیره شده را هم به صورت دستی پاک کرد. برای این کار باید وارد بخش Manage Website Data شوید تا کوکی‌های باقی‌مانده از وب‌سایت‌های مختلف را ببینید. برای پاک کردن هر ردیاب، روی گزینه Remove در کنار آن کلیک کنید. همچنین می‌توانید با کلیک کردن روی گزینه Remove All همه کوکی‌ها و ردیاب‌های ذخیره شده را پاک کنید.

کاربران اینترنت در جهان از کدام مرورگرها استفاده می‌کنند؟



این روزها اپل و گوگل

در حال رقابت برای به

دست آوردن مرورگرها

هستند، گوگل به

شدت به دنبال ایجاد

یک وب تعاملی برای

رقیب برنامه‌های بومی

است و اپل با سرعت

آهسته‌تری پیش

می‌رود



چطور از حریم خصوصی مان در مرورگرهای مختلف حفاظت کنیم؟

در جست‌وجوی امنیت



مسعود تیموری

روزنامه‌نگار

این روزها بالا بردن امنیت و حفظ حریم خصوصی کاربران در بین سازندگان مرورگرها در اولویت اول قرار گرفته است. با وجود این بعضی پیش می‌آید همین مرورگرها در مبارزه با هکرها و ردیاب‌های تبلیغاتی در دنیای شکست بخورند. در این گزارش قصد داریم آموزش دهیم چگونه تنظیمات حریم خصوصی خود را ارتقا دهید تا از نشت اطلاعات تان جلوگیری شود.

می‌شود؛ غیرفعال کردن GPS مرورگر و موتور جست‌وجو، خاموش کردن خودکار گذرواژه و حذف مرتب تاریخچه مرورگر را شامل می‌شود. اما اگر می‌خواهید حریم خصوصی خود را به سطح بالاتری برسانید ادامه این گزارش را تا انتها بخوانید.

گوگل کروم

طی سال‌های اخیر این تصور ایجاد شده که گوگل کروم به عنوان محبوب‌ترین مرورگر در جهان به حریم خصوصی کاربران خود بی‌تفاوت است. این درحالی است که این شرکت به توسعه دهندگان خود این امکان را داده تا با افزونه‌های مختلف روی این موضوع تمرکز کنند. به همین دلیل می‌توان گفت افزونه‌ها، یکی از اصلی‌ترین راهکارها برای افزایش و بهبود حفاظت از حریم خصوصی کاربران در گوگل کروم به شمار می‌آید. برای نصب افزونه‌های کروم، می‌بایست ابتدا وارد وب استور کروم شوید و سپس در سمت چپ، روی گزینه Extensions کلیک کنید. سپس با وارد کردن نام افزونه مورد نظر خود در نوار جست‌وجو، می‌توانید آن را پیدا کنید و در گوگل کروم نصب کنید. برای نصب تنها لازم است در صفحه اختصاصی هر افزونه، روی گزینه Add to Chrome را کلیک کنید. تنها لازم است در صفحه اختصاصی هر افزونه، روی گزینه Add to Chrome را کلیک کنید. Cookie Autodelete، uBlock Origin، HTTPS Everywhere، Privacy Badger جمله بهترین افزونه‌هایی است که به بالا بردن امنیت و حریم خصوصی کاربران کمک می‌کند. ناگفته نماند اگر مرورگر گوگل کروم در اندروید یا iOS استفاده می‌کنید، امکان استفاده از این افزونه‌ها را ندارید. برای حفاظت بهتر در این شرایط پیشنهاد می‌شود از مرورگرهای دیگری روی گوشی خود استفاده کنید.

موزیلا فایرفاکس

در مرورگر موزیلا، تنظیمات حفظ حریم خصوصی به مراتب بهتر و کاربردی‌تر مرورگرهای دیگر مثل کروم و اج است. برای بالا بردن حریم خصوصی در موزیلا، از منوی این مرورگر یا منوی سه خطی در بالا و سمت راست نوار ابزار، وارد بخش Preferences شوید. سپس گزینه Privacy & Security را انتخاب کنید. حالا در پنجره تنظیمات حریم خصوصی می‌توانید سه گزینه Standard و Strict و Custom را انتخاب کنید. تنظیمات پیش فرض مرورگر بر روی Standard است. این حالت، ردیاب‌ها را در تب‌های شخصی (حالت Private) غیرفعال می‌کند. علاوه بر این کوکی‌های شخص ثالث تبلیغاتی و استخراج‌کننده‌های رمزارز را هم غیرفعال می‌کند. حالت Strict، حالتی پیشرفته‌تر

بررسی مشکلاتی مثل نشت اطلاعات کاربران فیسبوک و توییتر و... نشان داده اغلب این اطلاعات از مرورگر کاربران به بیرون درز کرده است. نحوه جمع‌آوری داده‌های مختلف شرکت‌ها هنگام استفاده از اینترنت، باعث شده محافظت از حریم خصوصی کاربران به دغدغه اول نخبه‌های سیلیکون ولی تبدیل شود. این روزها اپل و گوگل در حال رقابت برای به دست آوردن مرورگرها هستند، گوگل به شدت به دنبال ایجاد یک وب تعاملی برای رقیب برنامه‌های بومی است و اپل با سرعت آهسته‌تری پیش می‌رود و همان‌طور که گفته شد بالا بردن امنیت و حفظ حریم خصوصی بعد دیگری به رقابت شرکت‌ها و تصمیم‌گیری کاربران برای استفاده از مرورگرها بخشیده است. شرکت اپل حریم خصوصی را در همه محصولات خود از جمله مرورگر سافاری در اولویت اصلی خود قرار داده است. مرورگر Brave هم حریم خصوصی را یک هدف اصلی برای تبلیغات خود تعیین کرده است. موزیلا و مایکروسافت هم اخیر در تبلیغات خود حفظ حریم خصوصی را به عنوان وجه تمایز خود با مرورگر گوگل کروم معرفی می‌کنند. مهندسان گوگل کروم اما به‌رغم اعتماد شرکت گوگل به درآمد تبلیغات، شروع به ساخت sandbox برای ارتقا حریم خصوصی کرده‌اند. برای همه مرورگرهای ذکر شده در این گزارش می‌توانید با تغییر موتور جست‌وجو و پیش فرض حریم خصوصی خود را افزایش دهید. به طور مثال DuckDuckGo را امتحان کنید. اگرچه ممکن است نتایج جست‌وجوی این مرورگر به اندازه گوگل برایتان مفید و عمیق نباشد، ولی به دلیل امتناع از ردیابی جست‌وجوهای کاربر، به شدت مورد علاقه کاربرانی است که به حریم خصوصی خود اهمیت می‌دهند. مواردی که معمولاً باعث افزایش حریم خصوصی