

google security ♦

امنیت

مترجم: محمدرضا رشیدی  
طراح و صفحه آرا: ویدا غلامی



کاری از کتابخانه ی :

گویا آیت

مقاومت ترین مجله اینترنتی ...

## فهرست مطالب

۴.....	شناسنامه کتاب.....
۵.....	سخنی با خوانندگان محترم.....
۶.....	افزایش ضریب امنیت در وب.....
۷.....	کلمات عبور(پسوردها).....
۱۰.....	کلاهبرداری با نامه ها و وب سایت های جعلی.....
۱۲.....	بدافزارها.....
۱۵.....	سایت های امن.....
۱۶.....	شبکه های امن.....
۱۶.....	امنیت موبایل.....
۱۷.....	واکاوی حساب Gmail.....
۱۸.....	امنیت خانواده.....
۱۹.....	تضمین امنیت خانواده در محیط آنلاین.....
۲۲.....	خارج شدن از حساب های کاربری.....
۲۳.....	ابزار های امنیتی گوگل.....
۲۶.....	اطلاعات شما در وب.....
۲۸.....	Cookies-کلوچه های هوشمند.....
۲۹.....	آدرس های IP.....
۲۵.....	حساب های کاربری.....

- ۳۰.....اطلاعات شما در گوگل
- ۳۱.....اطلاعات جستجو (لاگ ها)
- ۳۷.....حساب های گوگل و تاریخچه ی وب
- ۳۸.....موقعیت
- ۴۱.....بهبود نتایج جستجو
- ۴۵.....افزایش سرعت جستجو
- ۴۸.....Google Correlate
- ۴۹.....اطلاعات خود را مدیریت کنید
- ۵۰.....داشبورد گوگل
- ۵۰.....Ads Preferences Manager
- ۵۲.....انتقال اطلاعات با فاکتور آزادی و امنیت
- ۵۳.....خصوصی سازی جستجو
- ۵۴.....Google Talk
- ۵۵....."من دروب"
- ۵۷.....حالت Incognito در کروم
- ۵۸.....Google + و دکمه +
- ۵۸.....Google Docs
- ۵۹.....Latitude

امنیت گوگل

عنوان کتاب

گوگل

مؤلف

محمدرضا رشیدی

مترجم

ویدا غلامی

طراح جلد و صفحه آرا

کتابخانه گویا آی تی

محل انتشار



هرگونه دخل و تصرف در محتوای کتاب و همچنین سوء استفاده از مطالب، شرعا و قانونا جایز نیست.

سخنی با خوانندگان محترم

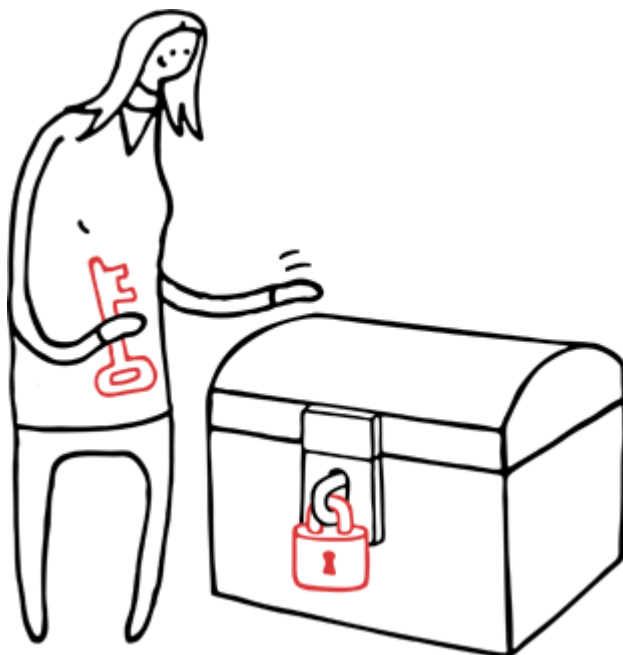
خدا را سپاسگذارم که فرصت مجدداً محیا شد تا با دومین کتاب در خدمتتان باشم. اگر از طرفداران پر و پا قرص گویا آی تی هستید و یا به هر نحوی کتابچه راهنمای آندروید را مطالعه نمودید؛ باید بگویم علی رغم محدودیت هایی که پیش رو داشتیم و همچنین تعجیل در انتشار کتاب، سعی کردیم تا کتاب در بهترین شرایط به دست شما عزیزان برسد که آرزومندیم به این مهم جامه عمل پوشانده باشیم. همچنین در این جا باید از جناب آقای میری، مدیر مجله اینترنتی گویا آی تی، که در واقع استارت کار از سوی ایشان بود نهایت تشکر را به عمل بیاورم. طراحی جلد و صفحه آرای نیز بر عهده خانم ویدا غلامی بود که علی رغم این که تجربه اول ایشان در این زمینه بود، اما بسیار عالی عمل کردند. از ایشان نیز نهایت تشکر را دارم.

و اما این کتاب که هم اکنون در اختیار شماست، با دقت و حساسیت بیشتری مواجه شد تا میزان کاستی ها و اشکالات را به حداقل برسانیم و حتی الامکان سعی کردیم تا هرازگاهی در میان مطالب، از طنز استفاده کنیم تا ذهن شما عزیزان در طول مطالعه، خسته نشود!

مطمئناً با مطالعه این کتاب به درک عمیق تر و متفاوتی نسبت به قبل از امنیت دست پیدا خواهید کرد و دید وسیع تری از آن خواهید داشت. گوگل، می داند چه بنویسد تا با ذهن ما و شما سازگار باشد به همین دلیل فکر می کنم کتاب پیش رو، متفاوت ترین کتاب امنیتی خواهد بود که تا به حال مطالعه کرده اید! در پایان از شما عزیزان و صاحب نظران درخواست می کنم تا بعد از مطالعه این کتاب، نسبت به ارسال بازخورد ها، انتقادات و پیشنهادات سازنده خود دریغ نفرمایید و این بنده را در جهت بهبود کیفیت کتاب ها یاری کنید.

## افزایش ضریب امنیت در وب

Page | 6



همه ی ما می دانیم که وب پر از مطالب جذاب و حتی متحیر کننده است، اما در مواقعی هم می تواند ترسناک باشد! مقوله ای که در این کتاب می خواهیم به آن بپردازیم، **امنیت** است که می گوید: "درست مانند دنیای حقیقی، باید از خود محافظت کنید و مانع از دزدیده شدن یا صدمه خوردن اموالتان شوید." فرقی نمی کند که تازه کار باشید یا خوره ی کامپیوتر؛ مهم این است که همیشه با نکات و مسائل پرداختن به اطلاعات در وب بروز باشید. در این کتاب، نکات بسیار مهم امنیتی ارائه خواهد شد که با رعایت آن ها می توان با خیال آسوده تری به وب گردی پرداخت.

## کلمات عبور (پسورد ها)

استفاده از کلمات عبور، اولین خط از انشای امنیت در برابر مجرمین سایبری است. کلمات عبور شما در حالی که از ضریب امنیتی بالایی برخوردار هستند، باید برای هر یک از حساب ها منحصر به فرد باشند و به طور مرتب عوض شوند.

Page | 7

### ۱- برای هر یک از اکانت های خود، پسورد منحصر به فردی انتخاب کنید.

مطمئناً شما هم تعداد زیادی اکانت در گوشه و کنار وب دارید و مسئله امنیت آن ها هم دغدغه ای برای شما به حساب می آید. پس، سعی کنید برای هر یک از اکانت های خود، مانند ایمیل یا حساب بانکی، پسورد منحصر به فردی انتخاب کنید. متخلفین این حوزه (!)، سایت هایی را که از ضریب امنیتی خوبی برخوردار نیستند، هدف می گیرند و سپس از نام های کاربری و پسورد های آن سایت برای سایت های دیگر استفاده می کنند. وقتی شما از پسورد های یکسانی برای اکانت های خود استفاده می کنید، این مجرمان، با پیدا کردن پسورد شما، قادر خواهد بود به همه ی اکانت های شما دسترسی پیدا کنند.

### ۲- از یک پسورد طولانی استفاده کنید.

هر چه پسورد شما طولانی تر باشد، حدس زدن مشکل تر خواهد بود؛ تازه تنها اگر شامل حروف و اعداد شود! کمی حوصله به خرج دهید و حداقل یک پسورد ۸ کرکتری انتخاب کنید.

### ۳- از ترکیب حروف، اعداد و نشانه ها در پسورد خود استفاده کنید.

استفاده از ترکیب حروف، اعداد و نشانه ها، امکان حدس زدن و هک کردن پسورد را کاهش می دهد. می دانید که با تنها ۸ کرکتر، چه طیف وسیعی از پسورد های ممکن روبروی شما خواهد بود؟

### ۴- از عبارات خاص استفاده کنید.

بعضی از پسورد ها به راحتی قابل تشخیص هستند. کلمات ساده یا عباراتی مثل : "password" و یا "letmain"، الگو های کیبورد مثل "qwerty" یا "qazwsx"، "abcd1234" و یا اطلاعات شخصی مانند

تاریخ تولد و ... بنابراین از ترکیبی از حروف، اعداد و نشانه ها در پسورد خود استفاده کنید تا بدین ترتیب، پسوردی منحصر به فرد داشته باشید که هیچ ربطی هم به اطلاعات شخصی شما نداشته باشد.

یکی از ایده های جالب، استفاده از عبارات خاصی است که در فیلم ها و یا موسیقی ها بکار برده می شوند و کمی غیر معمول هستند، مانند : "To be or not to be : That is the question". صبر کنید! حالا باید از نشانه ها، اعداد و .. استفاده کنید تا این عبارت را تبدیل کنید : "2bon2bt!tq". هر چه پسورد عجیب و غیر معمولی باشد، بهتر است! روش دیگر، استفاده از عبارات و کلمات رندوم و اضافه کردن اعداد و حروف به اول آن است، مانند : "spo0jdkl@xklcmvk".

#### ۵- مطمئن شوید راه های بازیابی پسورد تان روبراه و بروز هستند.

از روبه راه بودن آدرس ایمیل بازیابی پسوردها مطمئن شوید تا اگر مجبور شدید پسوردها را ریست کنید، خاطرتان جمع باشد. گاهی اوقات هم امکان وارد کردن شماره موبایل برای دریافت کدهای متنی وجود دارد. بر علاوه، بیشتر وب سایت ها (مانند Google Accounts) از شما درخواست انتخاب یک سوال امنیتی می کنند که در صورت فراموشی پسورد، برای شناسایی هویت شما از آن استفاده می کنند. در این باب، باید سوالی را انتخاب یا ایجاد کنید که پاسخ آن را فقط و فقط خودتان بدانید یا حداقل آن را به روش هایی که قبل گفته شد، مرتب کنید تا حتی اگر کسی پاسخ آن را به هر صورتی بدست آورد، دماغش بسوزد!

#### ۶- پسوردهایتان را در جایی امن نگاه دارید.

هرگز پسوردهایتان را بر روی کاغذ های یادداشت و .. ننویسید. اگر می خواهید پسوردهایتان را در کامپیوتر ذخیره کنید، نامی نامربوط به پوشه آن بدهید تا دیگران را گمراه کرده باشید! پیشنهاد من به شما این است که حتی الامکان پسوردهایتان را حفظ کنید، اما اگر آدم فراموش کاری هستید و یا مشغله کاری به شما این اجازه را نمی دهد، میتوانید از نرم افزارهای یادآورنده ی پسورد مثل lastpass استفاده کنید که با کمی جستجو در نت پیدا می شود.



## ۷- لایه های امنیتی حساب گوگل خود را افزایش دهید.



تصور کنید ؛ وقتی از خانه خود خارج می شوید، حس خوبی از قفل بودن در دارید. حالا اگر حفاظی هم تعبیه کرده باشید که نور علی نور! همین قضیه در مورد Google Account صدق می کند. با استفاده از " 2-step verification"، خیالتان را از بابت امنیت راحت کنید.

وقتی پسورد Google Account خود را وارد کردید، با فعال کردن قابلیت "2-step verification" می توانید یک لایه به لایه های امنیتی اضافه نمایید. این قابلیت، کاربر را در هنگام ورود به حساب، ملزم به داشتن دسترسی به گوشی موبایل می کند. این به این معنی است که اگر آدم "بووووووی" پسورد حسابتان را به هر نحوی بدست بیاورد، قادر نخواهد بود تا به حساب شما وارد شود، چون گوشی موبایل شما دست خودتان است و او باید بر علاوه بر پسورد باید گوشی شما را هم بدزدد! بنابراین، امنیت دو لایه خواهد داشت : لایه ای که آن را می دانید ( پسورد ) و لایه ای که آن را در اختیار دارید ( گوشی موبایل ).

## کلاهبرداری با نامه ها و وب سایت های جعلی ( فیشینگ )

کلاهبرداران اینترنتی به منظور سرقت مالی، صرف نظر از این که شما را می شناسند یا نه، تلاش می کنند اطلاعاتتان را بدزدند؛ اکثرا با جا زدن خود به جای افراد معتبر و دریافت اطلاعات شخصی شما. این طور وب سایت ها، وانمود می کنند که منبعی معتبر هستند، مانند بانک ها و یا حتی گوگل و بر این اساس تلاش می کنند تا شما را گول بزنند تا شما اطلاعات شخصی تان را با دست خودتان به آن ها تحویل دهید. (صفحات ورود به حساب کاربری یا همان لاگین) بنابراین، باید در بررسی این گونه صفحات آخرین دقت خود را بکار گیرید و همیشه از پیام هایی که از شما درخواست ارسال اطلاعات شخصی می کنند سرسری رد نشوید.

وب سایت ها و پیام های فیشینگ ممکن است از شما درخواست وارد کردن اطلاعات زیر را بکنند :

- نام های کاربری و پسورد ها
- شماره های اجتماعی امنیتی
- شماره حساب های بانکی
- کد های PIN ( شماره های شناسایی شخصی)
- شماره کارت های اعتباری
- نام خانوادگی مادران بعد از ازدواج
- تاریخ تولد شما

و می رسیم به نکاتی که باید برای محافظت خود از این گونه حملات، آن ها را رعایت کنید:

- ۱- مهم ترین نکته، پاسخ ندادن به ایمیل ها، توییت ها و پست های مشکوک حامل اطلاعات شخصی و مالی شما است. همچنین، به صفحات لاگین و فرم هایی که از این گونه پیام ها لینک شده اند اعتماد نکنید.
- ۲- هرگز پسوردتان را در صفحاتی که در ایمیل ها لینک شده اند وارد نکنید. حتی المقدور مستقیما به سایت مورد نظر بروید.

۳- پسورد تان را از طریق ایمیل ارسال نکنید.

۴- فقط و فقط هنگامی که ۱۰۰٪ مطمئن شدید در سایت معتبر و واقعی هستید، اقدام به وارد شدن به حسابتان بکنید. اگر مطمئن نبودید، آدرس سایت مورد نظر را در نوار آدرس مرورگر چک کنید. به طور مثال، این یک آدرس جعلی است :  
www.goog.le.com

۵- مرورگر تان را با بروزرسانی هایی که برای آن ارائه می شود، بروز نگاه دارید یا از مرورگر Chrome که اتوماتیک بروزرسانی می شود، استفاده کنید. اکثر مرورگر ها در هنگام ورود به سایت های مشکوک به کلاهبرداری به شما اخطار می دهند که در این باب، Google یک Safe Browsing API را ارائه کرده است که در فایرفاکس ، سافاری و کروم از آن استفاده می شود. ما (گوگل) هزاران صفحه وب را در روز آنالیز می کنیم و در سال، صد ها هزار از این وب سایت های فیشینگ را شناسایی و به بلک لیست Safe Browsing API اضافه می کنیم تا کاربران را از دسترسی به این وب سایت ها بازدارد.

۶- بیشتر سرویس دهندگان ایمیل، که شامل Gmail هم می شود، به شما امکان گزارش ایمیل های مشکوک و کلاهبرداری را می دهند. به این ترتیب با گزارش یک ایمیل، دیگر از طرف فرستنده آن ایمیلی دریافت نخواهید کرد و همچنین تیم ما طبق گزارش، تلاش می کنند تا حملات مشابه را بلاک کنند.

## بدافزارها

مفهوم "بدافزار"، تمامی نرم افزارهای مشکوک و مخرب طراحی شده برای ضربه زدن به کامپیوتر و یا شبکه را پوشش می دهد. بدافزارها می توانند بر روی دستگاه شما نصب شوند بدون اینکه حتی روح شما هم خبردار شود؛ اغلب توسط لینک های فریبنده و دانلود هایی که شما بدان علاقه دارید. به محض این که بدافزار بر روی دستگاه شما قرار گرفت، کلاهبرداران اینترنتی قادر خواهند بود تا به اطلاعات شخصی شما دسترسی پیدا کنند. چگونه؟! از طریق زدن رد کیبورد یا مانیتورینگ فعالیت های کامپیوتر! در این هنگام، کامپیوتر شما توسط فرد مورد نظر کنترل خواهد شد، وب سایت های مختلف را باز خواهد کرد، ایمیل های اسپم ارسال خواهد کرد و یا هر عمل دیگری را بدون اطلاع شما به انجام می رساند. به طور کلی، اعمال خطرناکی به طور زیرپوستی در بطن کامپیوتر شما انجام خواهد شد.

مثال هایی از بدافزار ها :

ویروس:

برنامه ای کامپیوتری که خود به خود تکثیر پیدا می کند و کامپیوتر را آلوده می کند.

کرم:

بدافزار کامپیوتری که اتوماتیک همانند سازی می کند و از کامپیوتر استفاده می کند تا کپی هایی از خودش را بین دیگر کامپیوتر های شبکه پخش کند.

**Spyware**:

بدافزاری جاسوسی که اطلاعات را بدون اطلاع کاربر جمع آوری می کند.

**Adware**:

پکیج های نرم افزاری که تبلیغات را بر روی کامپیوتر به طور اتوماتیک پخش، نمایش و دانلود می کنند.

اسب های تروجان:

برنامه ای مخرب که خود را به عنوان یک نرم افزار جا می زند. در این روش، نرم افزار در اول عملکردی قابل قبول را برای کاربر به نمایش می گذارد، اما کم کم اطلاعات را سرقت و به سیستم ضرر می رساند.

**در این جا به نکاتی اشاره می کنیم که باید برای محافظت خود در برابر بدافزارها، آن ها را رعایت کنید:**

- ۱- ورژن نرم افزار ها و سیستم عامل را ارتقاء دهید و اگر برایتان ممکن است، آپدیت های اتوماتیک را فعال کنید و برای نرم افزارهایی که آپدیت های اتوماتیک را ارائه نمی دهند، به طور دستی اقدام به بروزرسانی آن ها کنید.
- ۲- مراقب تک تک کلیک ها و دانلودهایتان باشید. تنها با یک کلیک بر روی لینک های مشکوک، کامپیوتر شما به وب سایت ها و نرم افزار های کلاهبرداری معرفی خواهد شد. این نرم افزار ها شامل برنامه هایی هستند که کامپیوتر شما را لحظه به لحظه اسکن می کنند و رد کلید هایی را که تایپ می کنید (مانند پسورد ها) می زنند. برای در امان ماندن از این حملات، تنها از منابع معتبر دانلود کنید و قبل از کلیک بر روی لینک ها، آدرس آن ها را چک کنید (با نگه داشتن کرسر موس بر روی آن لینک).
- ۳- هنگام گیر کردن در سایت های مشکوک و به ظاهر ناآشنا، سریعاً سایت را ترک کنید و از منابع دیگر نرم افزار مد نظر خود را دانلود کنید.
- ۴- هرگز به ایمیل هایی که ذره ی کمی هم مشکوک به نظر می رسند اعتماد نکنید. حتی ایمیل های دوستانتان هم اگر هک شده باشند، می توانند حاوی بدافزارها باشند. پس باید کاملاً مراقب لینک هایی که در ایمیل ها ارائه می شوند باشید. همان طور که قبل هم گفتیم، بهتر است آدرس وب سایت ها را مستقیماً وارد کنید.
- ۵- بعضی از برنامه ها بسته ای حاوی بدافزار ها و نرم افزارهای جاسوسی اینترنتی دارند که به عنوان قسمتی از پروسه ی نصب ایفای نقش می کنند. در هنگام نصب نرم افزارها، به پیام ها دقت کنید! بهتر است قبل از نصب کمی در مورد آن نرم افزار و نظرات دیگران تحقیق کنید. نهایتاً اگر نگران شدید، پنجره ی نصب را فوراً ببندید. هرچه باشد، امنیت حرف اول را می زند.

- ۶- ممکن است دوستان، آشنایان یا همکارانتان به شما یک فلش مموری یا دیسکی بدهند که آلوده باشد. حتما این جور وسایل را قبل از استفاده، اسکن کنید. این جاست که داشتن یک آنتی ویروس خوب و قانونی، به کمک شما می آید.
- ۷- هرگز به پنجره های پاپ- آپ که به شما داندلودی را ارائه می دهند اعتماد نکنید. حتی ممکن است در بعضی مواقع این پنجره های مزاحم، به شما بگویند کامپیوترتان آلوده شده است و باید برای پاک سازی آن، نرم افزاری را داندلود کنید. در این مواقع، پنجره را ببندید و هرگز در داخل آن کلیک نکنید.
- ۸- در به اشتراک گذاری فایل ها نهایت دقت را مدنظر قرار دهید. بیشتر سایت ها بدافزار خورشان(!) خوب است و باید در هنگام داندلود فایل ها احتیاط کنید. بدافزار ها می توانند در قالب یک ویدئو، موزیک یا نرم افزار به شما ضربه بزنند.
- ۹- در نهایت، هرچه زود تر از شر بدافزار ها خلاص شوید بهتر است. یا سیستم عامل تان را مجددا نصب کنید یا از نرم افزارهای امنیتی که در بازار هستند کمک بگیرید.

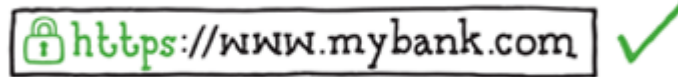
### پاک سازی بدافزارها

در حال حاضر، بهترین روش از بین بردن بدافزارها، استفاده از حداقل یک آنتی ویروس درجه ۱ و اسکن کامپیوتر بوسیله آن است. به علت محدودیت ها، نمی توانیم بر نقاط ضعف و قوت این نرم افزارها مانور بدهیم، اما امتحان این نرم افزار ها مجانی است! بهتر است به سایت [av-comparative.org](http://av-comparative.org) مراجعه و مقایسه آنتی ویروس ها را مشاهده کنید.

- [ESET Smart Security](#)
- [Kaspersky Lab Internet Security](#)
- [McAfee](#)
- [MacScan](#) (برای کاربران مک)
- [Microsoft Security Essentials](#)
- [Norton Internet Security](#)

## سایت های امن

## اطمینان از امن بودن سایت ها



تصور کنید وقتی به شعبه ای از بانک خود مراجعه می کنید، کارمندان آن جا را با نام هایشان، یونیفرم و سرویسی که به شما ارائه می کنند می شناسید. در رابطه با بانکداری الکترونیکی باید بگوییم که نیاز به اعتماد سازی، بیشتر از بانک های حقیقی حس می شود. پس بهتر است بدانید که سایت های امن با "https" شروع می شوند و آیکون یک قفل را در مرورگر ظاهر می کنند. با وجود این علائم، دیگر نباید نگران باشید.

## امن سازی ایمیل

مطمئننا شما هم دوست ندارید کسی به صندوق پستی خانه تان نگاه چپ بکند! پس این قضیه باید در مورد پست الکترونیکی تان هم صدق کند. Gmail، با ارائه ی درگاه امن HTTPS و 2-step verification به عنوان لایه ی بعدی امنیت، پیام ها و ایمیل هایتان از شر ویروس ها، Spyware ها و سایر بدافزار ها در امن و امان نگاه می دارد.

باز هم می گوییم: به علائم امنیت یک سایت (HTTPS و آیکون قفل) دقت کنید. این لینک را مشاهده کنید:

[How to ensure you connect to a safe network](#)

## شبکه های امن

در هنگام استفاده از شبکه های عمومی، مثل کافی نت ها، باید دقتی چند برابر را در نسبت با شبکه های محلی، چاشنی کار خود بکنید. سرویس دهنده های این گونه شبکه ها، می توانند تمام اطلاعات و ترافیک شبکه را که شاید اطلاعات شخصی شما هم جزو آن باشد، در مشت خود داشته باشند. وقتی می خواهید از طریق یک شبکه ی WiFi رمز نگاری شده که نیاز به پسورد ندارد، به نت متصل شوید (مانند کلید های WPA2)، افراد آن دوروبر قادر خواهد بود تا اطلاعات رد و بدل شده بین کامپیوتر شما و شبکه ی WiFi را ببینند.

اگر در خانه از WiFi استفاده می کنید، مطمئن شوید که از یک پسورد برای امنیت آن استفاده می شود. فقط کافی است دستورالعمل های ارائه شده توسط ISP یا سارنده ی Router را دنبال کنید تا پسوردی متمایز با پسورد پیش فرض سارنده (که مجرمان آن را از برند!) تنظیم کنید. همچنین ترجیحا از استاندارد WPA2 استفاده کنید.

## WiFi خانگی و امن!

فقط همین؛ باید برای شبکه های WiFi که استفاده می کنید، پسورد تنظیم کنید.

## امنیت موبایل

صرف نظر از کاربردی که موبایل برایتان دارد، حالا یا جستجو در وب یا دانلود نرم افزارها، همواره باید نکاتی را برای امنیت بیشتر در نظر بگیرید:

- ۱- از پسورد یا دیگر روش های قفل کردن گوشی استفاده کنید.
- ۲- هرگز اطلاعات شخصی تان را - مانند شماره PIN کات بانکی، هرگونه رمز عبور حساب ها و یا کد های امنیتی - در گوشی، پیام ها و یا ایمیل ها نگه داری نکنید. اگر مجبور شدید، از رمز و راز های خودمانی استفاده کنید!
- ۳- حتما قبل از دانلود نرم افزاری، دسترسی های آن را که بعد از نصب به گوشی شما خواهد داشت را بررسی کنید.



- ۴- حتما قبل از دانلود فایل، منبع آن را چک کنید تا از معتبر بودن آن خاطر جمع شوید. مثلا، اگر وارد لینکی با آدرس [www.googl.le.com](http://www.googl.le.com) شده اید که مطمئنا از گوگل سوءاستفاده کرده است، باید فوراً از آن لینک خارج شوید.
- ۵- وقتی می خواهید گوشی را بفروشید و یکی دیگر بخرید، حتما قبل از واگذار کردن گوشی، یک ریست بازگشت به تنظیمات کارخانه انجام دهید تا فایل های شخصی تان از روی آن پاک شوند.
- ۶- اگر گوشی مفقود شد، فوراً آن را گزارش دهید تا گوشی را از راه دور غیرفعال کنند و یا مکان آن را پیدا کنند.
- ۷- قابلیت آپدیت اتوماتیک را فقط برای نرم افزارهای مورد اعتماد فعال کنید.

## واکاوای حساب Gmail

اگر از جی میل استفاده می کنید، حتما نکات زیر را در نظر بگیرید:

- در تب "Mail Settings" تنظیمات forwarding و delegation (که به دیگران اجازه ی دسترسی به حساب شما را می دهد) را چک کنید. در آن جا، مطمئن شوید ایمیل های خروجی مستقیماً فرستاده می شوند.
- از بروز بودن ایمیل دوم، سوال امنیتی و شماره موبایل (برای بازیابی پسورد بر اساس SMS) اطمینان حاصل کنید: مطمئن شوید دسترسی تان به ایمیل دوم روبراه است؛ به گوشی دسترسی دارید و در صورت ارسال SMS آن را خواهید خواند و پاسخ سوال امنیتی را می دانید. وقتی مشکلی برای پسوردتان پیش بیاید، این روش ها به شما اجازه ی بازیابی آن را می دهند.
- به طور پیش فرض، حساب های Gmail از ارتباط امن HTTPS - وقتی از طریق یک شبکه بیسیم عمومی مثل هتل یا کافی نت می خواهید به حساب خود وارد شوید، این استاندارد به شما در حفاظت از اطلاعات در مقابل دزدیده شدن کمک می کند - استفاده می کند. شما می توانید این تنظیمات را طبق میل خود تغییر دهید.
- فعالیت های مشکوک در حساب خود را به طور مداوم بررسی کنید که این اطلاعات در پایین صفحه ضبط می شود که از مهم ترین آن ها می توان به شماره IP فردی که در حال استفاده از حساب است اشاره کرد.

## ایمنی خانواده

ما همه از اهمیت محافظت و آموزش قشر جوان که از اینترنت استفاده می کنند مطلع هستیم و می خواهیم آن ها تجربه ای امن از اینترنت را بدست آورند. در همین راستا، قابلیت هایی مانند SafeSearch و YouTube Safety Mode در اختیار خانواده ها قرار داده شده است تا بتوانند بر دسترسی اعضای خانواده کنترل بیشتری داشته باشند.

Page | 18

## جستجوی امن – SafeSearch



مطمئناً شما هم دوست ندارید وقتی یک کودک در حال استفاده از اینترنت است، نتایج ۱۸+ (!) در صفحات بدست بیاید! بنابراین، باید بدانید که قابلیت SafeSearch به شما این امکان را می دهد تا نتایج ۱۸+ را فیلتر کنید تا اعضای خانواده بتوانند شگفتی های نت را با آسایش و آرامش بیشتری واکاوی کنند!

و چون کودکان، کودک هستند و کنجکاو(!)، قفل SafeSearch این امکان را می دهد تا این فیلتر فقط با یک پسورد خاص از کار بیفتد!

## تضمین امنیت خانواده در محیط آنلاین

## ایمنی خرید

گوگل کالاها را از روش های مختلف به مشتریان عرضه می کند و اگر چه کنترل محتوای وب جایی در کار آن ندارد، مشتریان باید خرید هایشان را به صورت امن انجام دهند. اکثر تراکنش های آنلاین بدون مشکل انجام می شوند، اما خوب خطرهایی هم وجود دارد و این خطر ها، دلیل ارائه نکات زیر است.

## قبل خرید تحقیق کنید

- می دانید که همه به یک اندازه صادق نیستند و بعضا افرادی هم هستند که از صداقت بویی نبرده اند. قیمت کالایی که را می خواهید خریداری کنید، با جا های دیگر مقایسه کنید و در صورت وجود اختلاف قیمت قابل ملاحظه، با احتیاط پیش بروید.
- از فروشنده های مختلفی سوال کنید و اگر از فروشگاه های تا به حال خرید نکرده اید، در مورد سابقه آن جويا شوید تا اعتبار آن را سنجیده باشید. مثلا در اینترنت، نقد و بررسی های دیگر مشتریان را از خدمات فروشگاه مورد نظر بخوانید تا از صحت کار آن فروشنده با خبر شوید. معمولا فروشندگان معتبر اطلاعات تماسشان را در اختیار شما قرار می دهند تا در صورت وجود مشکل در تراکنش، آن ها را مطلع سازید. هرگز با فروشنده ای که تا به حال با آن برخورد نداشته یا در مورد آن چیزی نمی دانید، معامله نکنید و هواستان به کلاهبرداری های اینترنتی باشد.

## قبل از خریداری

- از روش های پرداختی که امنیت مشتریان را ضمانت می کند، استفاده کنید. کمپانی هایی که کارت اعتباری ارائه می دهند، معمولاً تعهدی در قبال کلاهبرداری های احتمالی ندارند. برای امنیت بیشتر، بعضی از سیستم های پرداخت آنلاین، مثل Google Checkout، شماره کامل کارت اعتباری شما را در اختیار فروشندگان قرار نمی دهد.
- قبل از خرید به نکاتی مانند نحوه ی ارسال کالا، گارانتی و فرصت تست محصول توجه کنید.

## نکات امنیتی و حریم خصوصی

### دریافت کالا

پرینت تراکنش را همواره نگاه دارید چون در مواقعی که می خواهید بازپرداخت انجام دهید و یا تراکنش های نامعتبر را گزارش دهید، به کمکشان خواهد آمد.

چک کنید تا مطمئن شوید کالایی که به دستتان رسیده، همانی است که برایش آن مقدار پول را پرداخت کرده اید؛ به محض این که کالا را دریافت کردید، سر وگوشی به آب دهید. هرچه زود تر نقص آن را متوجه شوید، راحت تر می توانید آن را پیگیری و به حق خود برسید!

### مبارزه با جعل کالا

هیچ کس دوست ندارد فریب بخورد تا کالایی جعلی خریداری بکند! کالاهای جعلی لوگویی مشابه با لوگوی اصلی آن کالا را دارند و با جعل آن لوگو، کالا را به عنوان کالای اصلی جا می زنند.

صاحبان برند و کاربران می توانند در صورت داشتن شکایت، در گوگل و در بخش Help Center، از راهنمایی های ان جا استفاده نمایند.

## گزارش تخلف از سرویس های گوگل

اگرچه گوگل مکانی برای تبلیغات و فروش کالا ها و ارائه ی سرویس ها است، اما کمپانی هایی هم وجود دارند تا تخلف های سهوی این شرکت را گزارش دهند:

Page | 21

- [AdWords](#)

- [AdSense](#)

- [Product Search and Merchant Center](#)

- [Checkout](#)

## کمک کمکی!

ارگان های متعددی در زمینه ی رسیدگی به شکایات کاربران و مشتریان فعالیت می کنند:

هر دو ارگان The Better Bussiness Burea و National Consumers League اطلاعاتی را ارائه می کنند. کمیسیون تجارت فدرال، ناظر این شکایات است.

اگر شکایت شما علیه شرکتی در خارج کشور است، می توانید در سایت [www.econsumer.gov](http://www.econsumer.gov) شکایت خود را مطرح کنید.

## خارج شدن از حساب های کاربری

تراکنش های مالی امن و سایت های مطمئن

Page | 22



تا حالا شده از خانه بیرون بزنید و پشت سر، در خانه را باز گذاشته باشید یا وارد حساب اینترنتی خود شده باشید و بعد از انجام کارتان، از آن خارج نشده باشید؟ شرایط وقتی بد تر می شود که از یک کامپیوتر به اشتراک گذاشته شده استفاده کرده اید!! حتما وقتی وارد حساب اینترنتی خود می شوید، بعد از اتمام فعالیت، از آن خارج شوید و پنجره ی مرورگر را ببندید.

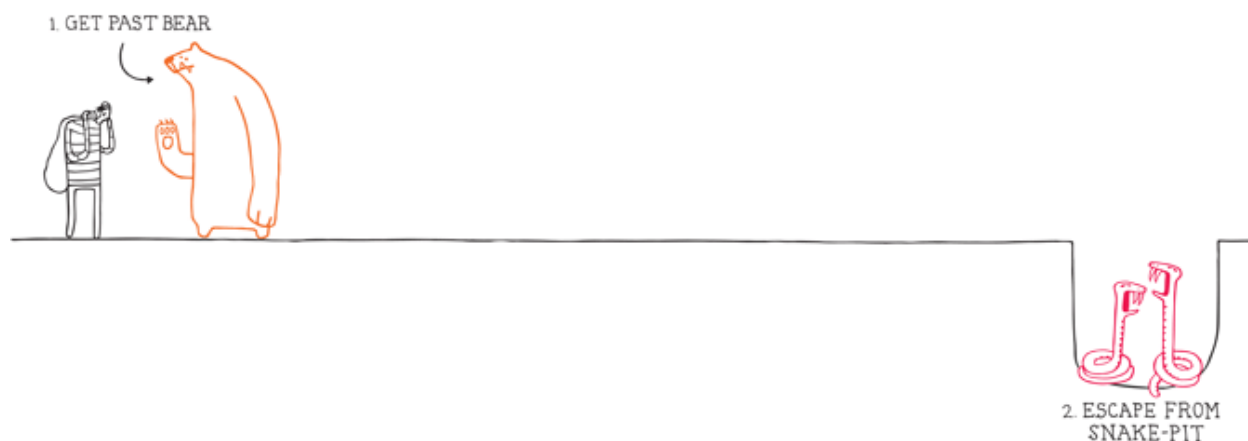
## ابزارهای امنیتی گوگل

در این جا به برخی از این ابزارها که امنیت کاربران را در وب افزایش می دهند، می پردازیم:

## 2-step verification (تأییدیه دو مرحله ای)

Page | 23

مطمئناً وقتی از خانه خارج می شوید، با قفل کردن درب، خیالتان راحت خواهد شد. تصور کنید؛ حالا اگر حفاظی برای درب هم تعبیه کرده باشید که نور علی نور خواهد بود! همین قضیه در مورد Google Account صدق می کند. با استفاده از "2-step verification"، دو لایه امنیتی از حساب شما حفاظت خواهد کرد.



همان طور که گفته شد، بعد از ایجاد پسورد برای حساب گوگل، می توانید با فعال کردن 2-step verification یک لایه ی ثانویه ی امنیتی را به حساب خود اضافه کنید. این لایه، شما را ملزم به داشتن دسترسی به گوشی موبایل می کند، اگرچه باز هم نیاز به نام کاربری و پسورد دارید. این به این معنی است که اگر آدم "بووووووقی" پسورد حسابتان را به هر نحوی بدست بیاورد، قادر نخواهد بود تا به حساب شما وارد شود، چون گوشی موبایل شما دست خودتان است و او باید بر علاوه بر پسورد، گوشی شما را هم بدزدد! بنابراین، امنیت دو لایه خواهد داشت: لایه ای که آن را می دانید (پسورد) و لایه ای که آن را در اختیار دارید (گوشی موبایل).

## رمزنگاری SSL جیمیل

Gmail، اولین سرویس دهنده ی ایمیل بود که رمزنگاری SSL را ارائه داد که با استفاده از آن، ایمیل های شما در مقابل صدماتی از قبیل دزدیده شدن یا ... محافظت می شوند. سپس این قابلیت گسترده تر شد به طوریکه سرویس های Picasa، Docs و ... از این قابلیت بهره مند شدند.

Page | 24

## وبگردی امن با کروم



یکی از مهم ترین کارهایی که می توانید برای افزایش ضریب امنیت در اینترنت انجام دهید، استفاده از یک مرورگر امن است. گوگل کروم یکی از این مرورگر هاست که از حریم شخصی شما حفاظت می کند و امنیت را برای شما به ارمغان می آورد. این مرورگر که قابلیت های زیادی دارد، از شما و کامپیوترتان در مقابل وب سایت های مشکوک و کلاهبردار محافظت می کند، از قبیل : Safe Browsing، Sandboxing و auto updates.



## Safe Browsing API

در این باب، Google یک Safe Browsing API را ارائه کرده است که در فایرفاکس، سافاری و کروم نیز از آن استفاده می شود. گوگل هزاران صفحه وب را در روز آنالیز می کند و در سال، صد ها هزار از این وب سایت های فیشینگ را شناسایی و به بلک لیست Safe Browsing API اضافه می کند تا کاربران را از دسترسی به این وب سایت ها بازدارد.

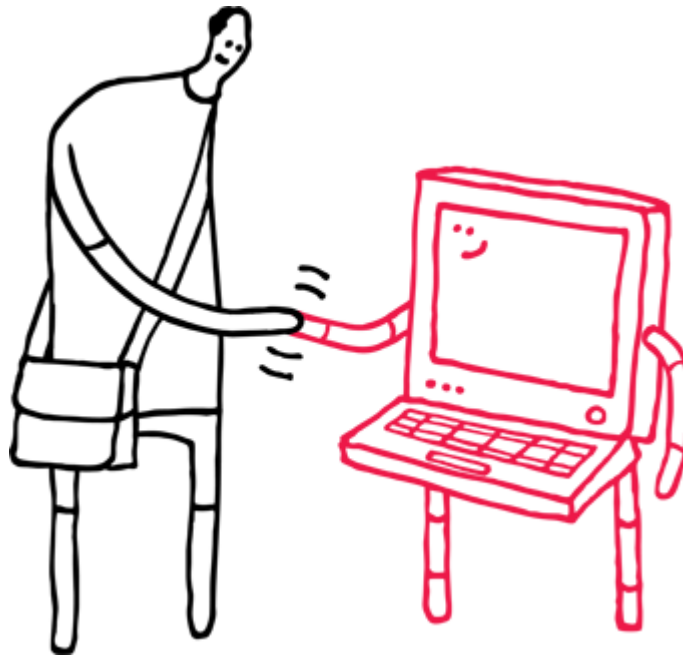
### هشدار دانلود های مشکوک در کروم

گوگل فکر همه چیز را کرده است و امنیت کاربران را در برابر بدافزارهایی که بوسیله دانلود بر روی کامپیوتر ها منتشر می شوند، مد نظر قرار داده است. Safe Browsing خدمات زیادی را به وب عرضه کرده است؛ وب با وجود تمامی این محتوای مضر، باز هم همان وب است!

ببینید، سایت های زیادی در این وب هستند که دانلود رایگان را برای شما فراهم آورده اند، اما به قیمت کلاهبرداری! این سایت ها بر خلاف آن چه که در ظاهر نشان می دهند، در کفش خود ریگی دارند. آن ها با استفاده از چرب زبانی های بصری، کاربران را فریب می دهند و آن ها را مجاب به دانلود و اجرای محتوایی که شامل بدافزار است می کنند. حالا قابلیتی در مرورگر کروم تعبیه شده است تا کاربران را از دانلود این گونه فایل ها (با فرمت اجرایی ویندوز)، باز دارد. این قابلیت وقتی با دانلود مشکوکی از سوی کاربر مواجه می شود، به او هشدار می دهد.

## اطلاعات شما در وب

Page | 26



هر صبح، به کافی شاپ همیشگی می روید و قهوه اسپرسو سفارش می دهید که با متود همیشگی سرو می شود. حتی دیگر کارکنان کافی شاپ هم قبل از ورود شما به آن جا می دانند چه چیزی می خواهید سفارش دهید! وب سایت هایی اعم از گوگل، می دانند اگر کاربر را بهتر بشناسند، بهتر می توانند به آن ها خدمت کنند.

EXTRA-HUGE  
TRIPLE-SHOT  
JUST THE WAY  
YOU LIKE IT



در اوایل پیدایش وب، صفحات ایستا خلق شدند که برای همه کاربران به یک شکل به نظر می رسیدند. این روز ها، وب کارآمد تر شده است، چون وب سایت ها دیگر می توانند شما را بشناسند و حدس بزنند چه چیزهایی را برای نمایش می پسندید. برای مثال، می توانند با استفاده از اطلاعاتی که قبلا مشاهده کرده اید، به یاد آورند شما چه زبانی را برای مشاهده آن ترجیح می دهید، چه کتاب ها و موزیک هایی را دوست دارید و چه آدرسی را برای خرید های اینترنتی استفاده می کنید که این اطلاعات ها در فایل هایی به نام **cookies** ذخیره می شوند. این کوکی ها، آدرس های IP و لاگین کردن به حساب های اینترنتی از نشانه های این قابلیت هستند.

## Cookies - کلوچه های هوشمند!

یکی از رایج ترین روش وب سایت ها برای به یاد آوری اطلاعات و ترجیحات شما، استفاده از cookie ها است. این کوکی ها، فایل های کوچک حامل اطلاعات هستند که در مرورگر زندگی می کنند و شما را از معرفی مجدد خود به وب سایت ها بی نیاز می کنند. به عنوان مثال، این فایل ها می توانند به موتورهای جستجو بگویند شما از چه زبانی برای جستجو استفاده می کنید و همچنین به فروشگاه های اینترنتی کمک کنند تا کالاهایی را که شما قبلا در سبد خرید قرار داده بودید، به یاد آورند. در سمت دیگر، بازاریاب با استفاده از این کوکی ها، می توانند تبلیغاتی را که بیشتر به شما مربوط است، نمایش دهند!

تمام مرورگر های مدرن امروزی قابلیت حذف یا بلاک کوکی ها را دارند. اما به این نکته توجه داشته باشید که بعضی از سایت ها یا بدون کوکی ها اجرا نمی شوند و یا به خوبی عمل نمی کنند. نمونه کوچکی از اطلاعاتی که می توانند در کوکی ها ذخیره شوند:

```
SITE:      GOOGLE.COM
CONTENT:   ID= 03b1d4f3936
           99771: LD=en:NR=10...
DOMAIN:    GOOGLE.COM
EXPIRES:    THU, NOV 26, 2013
           3:40:16 PM
```

نام: نام کوکی است که برای هر سایتی که آن را ست می کند منحصر به فرد است.

نام سایت: نام دامنه یا زیر دامنه ای که کوکی را ست کرده است.

تاریخ انقضا: بعد از تاریخ انقضا، کوکی ها اتوماتیک حذف می شوند. این در حالی است که بعضی از کوکی ها به هنگام بسته شدن پنجره مرورگر حذف می شوند و یا ماه ها و سال ها بعد از ست شدن پاک می شوند که این گونه کوکی ها، کوکی های پایدار نامیده می شوند.

یک مقدار: اطلاعاتی است که در کوکی ها که وب سایت با استفاده از آن ها شما را به یاد می آورد.

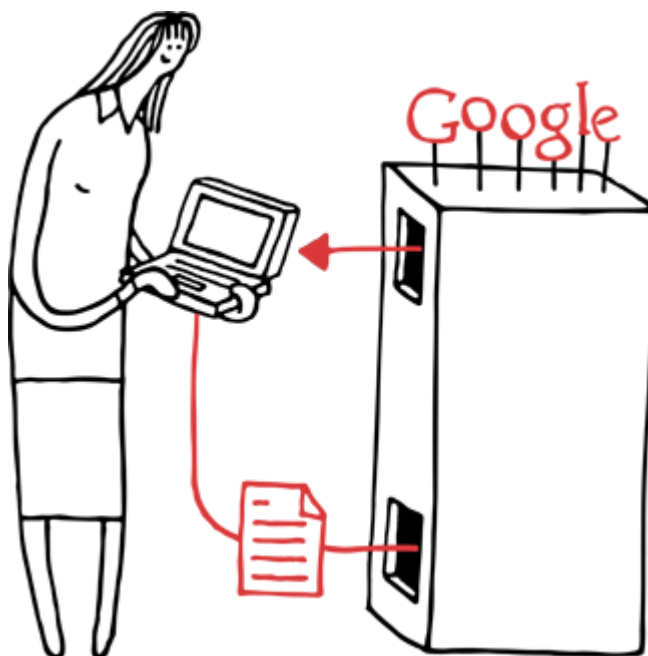
## آدرس های IP

**آدرس IP** کامپیوتر شما مانند شماره تلفن منزل شما می باشد! اگر کسی بخواهد با شما ارتباط برقرار کند، به شماره تلفن منحصر به فرد شما زنگ می زند. این قضیه در وب هم برقرار است. اینترنت با استفاده از آدرس IP کامپیوتر شما، صفحه وب درخواستی را به کامپیوترتان ارسال می کند. آدرس IP اغلب شامل اطلاعاتی درباره سرویس دهنده ی اینترنت شما (ISP) و موقعیت مکانی است و وب سایت ها می توانند با استفاده از این اطلاعات، مکان شما را تشخیص دهند. این به وب سایت این امکان را می دهد تا بتواند با اطلاع از IP شما، زبان مورد نظر شما را اتوماتیک تشخیص دهد و یا محتوایی را به شما ارائه دهد که مربوط به شما می شود.

## حساب های کاربری

راه دیگری که وب سایت ها با استفاده از آن شما را شناسایی می کنند، وارد شدن (لاگین) به حساب کاربری است. به محض این که لاگین کنید، سایت اطلاعات شما را فراخوانی می کند. این اطلاعات برای سایت های گوناگون مختلف است؛ مثلاً در یک وب سایت خرید، سبد خرید و یا آدرس پستی شما فراخوانی می شود. حتی کالاهایی که قبلاً توسط شما خریداری شده اند هم قابلیت نمایش پیدا می کنند و سایت می تواند بر اساس آن ها به شما پیشنهاداتی را ارائه دهد. به یاد داشته باشید هنگام ایجاد حساب کاربری، از پسورد مطمئن استفاده کنید.

## اطلاعات شما در گوگل



...وقابلیت هایی که سرویس های گوگل را مفید تر جلوه می دهند.

با دانستن اطلاعاتی درباره ی کاربران، گوگل می تواند سرویس هایش را مفید تر و مناسب تر و در خور کاربر به او ارائه دهد. مثلاً می تواند نتایج جستجوی ایده آلی برای شما نمایش دهد. این شرکت با آنالیز جستجو های میلیون ها کاربر، الگوریتم جستجویش را بهبود بخشد، قابلیت های جدیدی را ارائه دهد، امنیت بیشتری را فراهم آورد و حتی در مورد آینده پیش بینی کند!

و اما...جایی که حرف از نگهداری اطلاعات شما در گوگل در میان است، همواره امنیت و کنترل چاشنی کار این شرکت است.

این شرکت پنج اصل امنیتی و حریم خصوصی تدوین کرده است که نحوه ی محافظت از حریم خصوصی و اطلاعات کاربران را تشریح می کند:

۱- با استفاده از اطلاعات قبلی، کالاهایی معتبر و با ارزش به کاربر ارائه شود.

۲- طیف توزیع کالاهایی که از استاندارد های حریم خصوصی و امنیتی برخوردار هستند، افزایش یابد.

۳- مجموعه اطلاعات شخصی شفاف سازی شوند.

۴- به کاربران راه های محافظت از حریم شخصی ارائه شود.

۵- در برابر اطلاعاتی که نگهداری می کنیم، مسئول باشیم.

### ردپاهای جستجو (لاگ ها)

تاحالا به این فکر کرده اید که چه اتفاقی می افتد وقتی متن مورد نظر را در گوگل تایپ می کنیم و گوگل چه اطلاعاتی را در رابطه با آن جستجو ذخیره می کند؟

مثلا یک جستجوی ساده مثل "ماشین ها" را مثال می زنیم. وقتی کسی کلمه " ماشین ها را" در سیستم سرچ گوگل وارد می کند، آن جستجو از طرف سیستم کاربر به کامپیوتر های گوگل ارسال می شود و نتایج مطلوب تشکیل می شوند. وقتی کامپیوتر های گوگل نتایج را یافتند، آن ها را در کسری از ثانیه به کامپیوتر کاربر ارسال می کنند.

گوگل در این پروسه، اطلاعاتی را بدست می آورد : عبارت جستجو شده، زمان و تاریخ تایپ عبارت، آدرس IP و کوکی کامپیوتری که جستجو را انجام داده است، مرورگر و بالاخره سیستم عامل. این اطلاعات به عنوان "لاگ" تلقی می شوند و بسیاری از وب سایت ها از این قبیل اطلاعات را با روشی مشابه گوگل ذخیره سازی می کنند.

مثالی از یک لاگ جستجوی گوگل:

123.45.67.89 - 25/Aug/2011 10:15:32 -

http://www.google.com/search?q=cars-

Chrome 2.0.0.7; Windows NT 5.1-

740674 ce2123e969.

Page | 32

این ها به چه معنایی هستند؟

## آدرس IP:

123.45.67.89 یک آدرس IP است که از سوی سرویس دهنده ی اینترنت به کامپیوتر کاربر اختصاص داده می شود. درست مانند دیگر وب سایت ها، وقتی از گوگل درخواست صفحه ای را می کنید (یک صفحه نتایج)، گوگل با استفاده از آدرس IP کامپیوتر شما، نتایج را درست به کامپیوتر شما باز ارسال می کند.

باید بدانید که آدرس IP اطلاعاتی از قبیل مکان دقیق و هویت شما را ارائه نمی دهد. در حقیقت، بعضی از سرویس دهندگان اینترنت (ISP ها)، این امکان را به کاربران داده اند تا آن ها بتوانند در هر بار اتصال به اینترنت، آدرس IP متغیری را به خود اختصاص دهند. بیشترین اطلاعاتی که گوگل می تواند از طریق آدرس IP یک کاربر بدست آورد، مکان عمومی او (مانند Boston) و ISP که از آن اینترنت می گیرد، است. در این جا، نقش ISP خیلی پررنگ است چون تنها او می تواند IP ها را برای کاربران منحصر به فرد ست کند.

## زمان و تاریخ:

25/Aug/2011 10:15:32 تاریخ و زمان جستجوی عبارت توسط کاربر در گوگل است.



## جستار:

<http://www.google.com/search?q=cars> جستار است که در این جا عبارت "cars" جستجو شده

است.

Page | 33

## مرورگرها و سیستم عامل:

Chrome 2.0.0.7 Windows NT 5.1 مرورگر و سیستم عامل استفاده شده توسط کاربر است.

## کوکی:

740674ce2123a969

ID منحصر به فرد کوکی است که وقتی کاربر برای اولین بار سایت گوگل را باز می کند، در مرورگر ذخیره می شود. درست مثل یک آدرس IP، کوکی مکان دقیق و یا هویت اصلی شما را برای گوگل فاش نمی کند بلکه فقط یک کامپیوتر را شناسایی می کند. شما می توانید این کوکی ها را هر وقت که مایل بودید از طریق خود مرورگر حذف کنید!

## محدودیت نگهداری اطلاعات

گوگل بعد از ۹ ماه آدرس های IP را ناشناس می کند و همچنین شماره کوکی ها را نیز دائما تغییر می دهد. این کار، رابطه ای که بین جستار و کامپیوتر کاربر بود را از بین می برد و شبیه به روشی است که در آن شماره کارت اعتباری با علامت های دیگر جایگزین می شود تا امنیت مشتری افزایش پیدا کند.

این جا مثالی از یک IP که بعد از ۹ ماه توسط گوگل ناشناس شده است مشاهده می شود: 123.45.67.xxx. بعد از ۱۸ ماه، کوکی با کوکی دیگری که فقط اسمش عوض شده است جایگزین می شود.

گوگل اولین متور جستجو بود که محدودیت نگهداری لاگ های اطلاعات را پیشنهاد داد و به دنبال آن، شرکت های دیگر نیز از این پروسه در سیستم شان استفاده کردند.

درست مثل کلوچه هایی که در دنیای حقیقی (آفلاین) وجود دارد، کوکی های آنلاین نیز برای همیشه وجود نخواهند داشت! کوکی های گوگل بعد از ۲ سال منقضی می شوند. بر علاوه، گوگل همیشه به کاربر های خود این اجازه را داده است که حتی بدون کوکی، از سرویس ها استفاده نمایند، اما خوب مسلما اگر از کوکی ها صرف نظر شود، کاربر باید قید بعضی از سرویس ها و عملگر های خاص را بزند!

### دلیل نگهداری لاگ های جستجو

گوگل از لاگ های جستجو برای اهداف خاصی استفاده می کند. برای مثال، حفظ امنیت سرویس ها، توسعه قابلیت هایی که موتور جستجو را سریع تر و نتایج را بهبود می بخشد و حتی پیش بینی خطرات احتمالی!

اگر می خواهید بدانید در هنگام جستجو در گوگل، چه اطلاعاتی در لاگ ذخیره می شود، مطلب بعدی را از دست ندهید.

### تبلیغات

مطمئنا شما نیز از یک مجله که در آن به موضوع کلاهبرداری های اینترنتی پرداخته شده است، انتظار ندارید تا تبلیغاتی در رابطه با موسیقی و ویدئو نمایش بدهد. پرداختن به تبلیغاتی که برای خواننده یا بازدیدکننده ملموس تر و جذاب تر است، نتایج کاملا مطلوبی را خواهد داشت. در اینترنت هم، این نکته صادق است: وب سایت ها تلاش می کنند تا تبلیغاتی را نمایش دهند که جذاب تر و ملموس تر باشند و تا قسمتی نیز به موضوع وب سایت مرتبط باشد.

گوگل نیز سعی کرده است تا تبلیغات را متناسب با علاقه کاربران انتخاب نماید که این کار را با استفاده از اطلاعات کاربران انجام داده است؛ چه در موتور جستجو و چه در سرتاسر وب.

### جستجو

تبلیغاتی که در صفحه نتایج گوگل نمایش داده می شود، براساس جستار شما است. به طور مثال اگر عبارت "پرواز های ارزان" را در گوگل تایپ کنید، مطمئنا لینک های تبلیغاتی شرکت های هواپیمایی را خواهید دید. این که چه تبلیغاتی نمایش

داده شوند، سیستم اتوماتیک گوگل بر اساس موضوع جستار شما، میزان رابطه تبلیغات با آن و مقدار هزینه ای که مبلغ برای تبلیغ خود کرده است، آن را تشخیص می دهد. این پروسه از هیچ یک از اطلاعاتی که ممکن است با گوگل به اشتراک بگذارید (مانند جیمیل) استفاده نمی کند و رنکینگ تبلیغات ذره ای به نتایج طبیعی گوگل مربوط نیست.

نمونه هایی از تبلیغات که ممکن است با آن ها روبرو شوید:

### تبلیغات بر اساس علاقه

به جز لینک های حمایت شده که در صفحه نتایج گوگل می بینید، گوگل با اجرای نقشی به عنوان واسطه میان مبلغان و صاحبان سایت ها، تبلیغات را نمایش می دهد. این گونه تبلیغات بر اساس محتوای وب سایت های مرتبط به نمایش در می آیند. در موارد دیگر، این تبلیغات بر اساس علاقه خواهند بود و دلیل نمایش آن ها حدس هایی خواهند بود که گوگل در مورد علاقه شما خواهد زد! مثلاً یکی از فاکتور هایی که گوگل را در این حدس زدن ها کمک می کند، تاریخچه وب سایت هایی هستند که قبلاً از آن ها دیدن کرده اید. مثلاً هر چه بیشتر در مورد سایت های فضا سازی حساس شوید، تبلیغات بیشتری را در مورد آن خواهید دید.

پروسه ی نمایش تبلیغات ب صورت زیر است:

- وقتی به وب سایتی سر می زنید یا جایی ویدئویی را تماشا می کنید که گوگل تبلیغی را نمایش می دهد، گوگل با استفاده از یک کوکی، شماره ای را در مرورگر ذخیره می کند تا تعداد بازدید های شما محاسبه شود. این شماره می تواند مانند ۱۱۴۴۱۱ باشد.
- سپس، به دلیل این که بیشتر وب سایت هایی که به آن ها سر می زنید در مورد باغبانی است، گوگل شماره ی شما را (۱۱۴۴۱) در رده ی "علاقه مندان باغبانی" قرار می دهد.
- بنابراین در هنگامی که به جستجوی وب می پردازید، گوگل تبلیغات بیشتری را در مورد باغبانی به شما نمایش خواهد داد.

توجه داشته باشید که در این پروسه، گوگل هیچ نام و یا [اطلاعات شخصی](#) را نگه داری نمی کند. گوگل تنها شماره ای که در کوکی مرورگر شما ذخیره شده است را شناسایی می کند و بر اساس آن رده بندی، تبلیغاتی را به شما نمایش خواهد داد. پس گوگل مرورگر شما را شناسایی می کند، نه شما را! خاطر نشان می کنم که گوگل هیچ گاه تبلیغات را بر اساس اطلاعات حساسی مانند مذهب، نژاد، رفتارهای جنسی، سلامت و رده بندی های مالی نمایش نمی دهد.

شما می توانید نوع تبلیغاتی را که مشاهده می کنید را با استفاده از [Ads Preferences manager](#) تحت کنترل داشته باشید. تین به شما این امکان را می دهد تا رده بندی های علاقمندی را که در مرورگر شما ذخیره شده است، تغییر دهید و یا حتی اگر مایل نیستید این رده بندی ها ذخیره شوند، خواهید توانست آن را به طور کلی غیرفعال کنید.

## تبلیغات در Gmail

تبلیغاتی که در جیمیل نمایش داده می شود مشابه تبلیغاتی است که در گوشه و کنار صفحه نتایج جستجو نمایش داده می شود، با این تفاوت که معیار نمایش تبلیغات، نوع پیام هایی است که با آن ها سر و کار دارید. هدف گوگل این است که تبلیغاتی را به کاربران نمایش دهد که بیشتر مورد پسند کاربران قرا می گیرد.

این پروسه (Ad targeting) کاملاً به طور اتوماتیک انجام می پذیرد و دست هیچ انسانی در آن دیده نمی شود. مثلاً کسی نمی نشیند تا تک تک ایمیل های شما را بخواند و بر اساس آن ها برای شما تبلیغاتی را تنظیم کند! از این اسکن اتوماتیک در دیگر عرصه ها مانند مبارزه با اسپم و فیلترینگ ویروس ها و غلط یابی و نه تنها فقط بوسیله جیمیل، بلکه توسط دیگر سرویس دهنده ها، استفاده می شود.

تبلیغات با استفاده از تکنولوژی تبلیغاتی که [Google AdSense Program](#) هم از آن استفاده می کند، انتخاب و سرو می شوند!

باید بدانید که تنها تبلیغاتی از طریق شبکه محتوایی و جیمیل گوگل توزیع می شوند که در رده ی "سلامت برای خانواده" قرار گیرند. همچنین گوگل در مورد محتوایی که تبلیغات را برای آن ها تنظیم می کند، بسیار مراقب است. برای

مثال، گوگل ممکن است از به نمایش در آمدن تبلیغات در کنار یک ایمیل که در مورد خبری فاجعه آمیز است جلوگیری کند. بر علاوه، گوگل هیچ گاه تبلیغات را بر اساس اطلاعات حساسی مانند مذهب، نژاد، رفتار های جنسی، سلامت و رده بندی های مالی نمایش نمی دهد. شما می توانید از صفحه **Gmail Settings** خودتان کنترل اوضاع را بر دست بگیرید! اطلاعات بیشتر در [Help Center](#).

### حساب های گوگل و تاریخچه ی وب

وقتی شما یک [حساب کاربری](#) ایجاد می کنید، قادر خواهید بود تا با استفاده از حساب خود، تاریخچه ی وب را فعال کنید. بسیاری از مردم، مطالبی را در وب پیدا می کنند که بسیار به آن ها علاقه مند هستند، مثل یک ویدئوی جالب، دستور پخت یک شکلاتی، مقاله روزنامه و ...، اما بعد از گذشت چند روز از آن ها غافل می شوند و این یعنی از دست دادن آن ها. تاریخچه وب به شما این امکان را می دهد تا صفحات وبی را که در گذشته مشاهده کرده بودید را مشاهده کنید، مانند نتایج جستجوی گوگل. بنابراین می توانید آن مطالب مورد علاقه تان را دوباره مشاهده کنید. همچنین تاریخچه ی وب می تواند گرایش شما را به فعالیت های وب نشان دهد. مثلاً امار وب سایت هایی که از همه بیشتر مشاهده کرده اید یا جستجو هایی که در صدر جستجو های شما بوده اند!

استفاده از تاریخچه ی وب، همچنین به معنای دریافت نتایج مناسب تر و شخصی سازی شده است:

- شخصی سازی ورود به حساب

وقتی شما وارد حساب گوگل می شوید، گوگل بر اساس جستجو هایی که قبلاً انجام داده اید و یا وب سایت هایی که در گذشته از آن ها بازدید کرده اید، تجربه شما شخصی سازی می کند.

- شخصی سازی خروج از حساب

وقتی شما هنوز به حساب وارد نشده اید، گوگل بر اساس اطلاعات جستجو های قبلی شما که توسط کوکی ها در مرورگر ذخیره شده اند، تجربه جستجوی شما را خصوصی سازی می کند. گوگل آمار بیش از ۱۸۰ روز از فعالیت های جستجوی شما را که در کوکی مرورگر به آن اشاره شده است نگهداری می کند که شامل جستار ها و نتایجی که بر روی آن ها کلیک کرده اید می شود.

تاریخچه وب شما در سرور های گوگل نگهداری می شود، بنابراین می توانید آن را توسط هر کامپیوتر دیگری و تنها با وارد شدن به حساب گوگل خود، مشاهده و مدیریت کنید. ب خاطر داشته باشید که گوگل تنها اطلاعات صفحاتی که از آن ها بازدید می کنید را نگهداری می کند، مثل URL، و هیچ گاه تصویری از آن صفحات را در حساب نگهداری نخواهد کرد.

اما در صورتی که از این قابلیت خوشتان نمی آید، می توانید آن را به طور موقت یا دائمی غیر فعال کنید.

خوب است بدانید در هنگام استفاده از تاریخچه وب ( Web History )، نتایج جستجو چگونه شخصی سازی می شوند. تایپیک بعدی را بخوانید!

### موقعیت

با استفاده از اطلاعات موقعیت، گوگل می تواند محصولات را هماهنگ با آن منطقه عرضه و در واقع، کیفیت محصولات را بهبود بخشد. اما از آن جایی که این اطلاعات حساس هستند، با احساس مسئولیت بیشتری نسبت به آن اقدام می کند.

### My location ( موقعیت من ) در Google Maps

در [Google Maps](#) ( چه در ورژن موبایل و چه دسکتاپ ) قابلیتی به نام [My Location](#) وجود دارد که موقعیت شما را بر روی نقشه نشان می دهد. از مزایای این قابلیت می توان به این موارد اشاره کرد : ذخیره وقت و فهمیدن موقعیت دقیق خود، کسب اطلاعات از محیط اطراف و بالاخره نحوه رفتن از نقطه A به B. در ورژن دسکتاپ، گوگل مپ موقعیت شما را از طریق قابلیت جغرافیایی [مرورگر وب](#) می فهمد. بر روی موبایل، این کار از طریق خود گوشی انجام می پذیرد. برای

اطلاعات بیشتر می توانید [Google Maps Help Center](#) را ببینید یا به راهنمای موقعیت یابی مرورگر مراجعه کنید.

بار اول که از My Location استفاده می کنید، از شما سوال می شود که آیا می خواهید به گوگل اجازه دهید تا از اطلاعات موقعیت شما استفاده کند یا نه؟ گوگل با استفاده از آن نخواهد فهمید که شما که هستید و در حالی که اطلاعات اصلی را (اطلاعاتی که دقیقاً می گوید کاربری **ناشناس** در چه موقعیتی قرار دارد) ذخیره می کند، هیچ گاه اطلاعات شخصی و شناسایی را نگهداری نخواهد کرد. شما می توانید به طور دستی موقعیت خودتان را تعیین کنید و این کار الزاماً نباید اتوماتیک باشد. و همانطور که خودتان هم می دانید، گوگل تنها آخرین موقعیتی را که به Google Latitude ارسال می شود را در حساب گوگل ذخیره می کند، مگر این که خودتان نسبت به [Location History](#) (تاریخچه موقعیت ها) اقدام کنید.

## موقعیت و محصولات گوگل

در [Help Center](#) می توانید اطلاعات بیشتری را راجع به چگونگی استفاده گوگل از موقعیت شما کسب کنید.

خوب است بدانید گوگل چگونه از موقعیت شما استفاده می کند تا محصولاتش را کاربردی تر کند. تایک بعدی را بخوانید!

## محصولات دیگر گوگل و حریم شخصی

### مرورگر Chrome

گوگل کروم را تنها برای سریع بودن تولید نکرد، بلکه دادن اختیار به کاربر برای حفاظت از اطلاعات شخصی در نت، یکی از ملاک های مهم برای آن بود. کروم قابلیت های بسیاری را از قبیل حالت **Incognito** به شما عرضه می کند که با آن می توانید از حریم شخصی خود حفاظت کنید؛ این مرورگر با داشتن تنظیمات خاصی، به شما این امکان را می دهد تا بر کوکی ها، تصاویر، جاوا اسکریپت و پلاگین ها و ... مدیریت داشته باشید.

## Gmail

هدف گوگل از ایجاد جیمیل، بهبود تجربه ی استفاده از نامه الکترونیکی بود و این شرکت راه خودش را در مسیر خلق ایده های جدید برای هرچه بهتر کردن این تجربه ادامه خواهد داد که همواره توام خواهد بود با تلاش برای حفظ امنیت و حریم شخصی شما. Gmail طیف وسیعی از ابزار ها را از قبیل اسکن برای ویروس، مبارزه با اسپم ها، ارتباط امن HTTPS و تایید دو مرحله ای ( 2-step verification ) به شما ارائه می دهد.

## Google +

گوگل پلاس حریم شخصی را در اولین اولویت قرار داده است و با ارائه قابلیت های بی شماری که به شما امکان پست و به اشتراک گذاری مطالبی که به آن ها علاقه مند هستید را می دهد، در حال حاضر به یکی از محبوب ترین شبکه های اجتماعی تبدیل شده است.

## Street View

این ماشین گوگل خیلی جنجال به پا کرده است، اما خوب چیزی که در این بین به چشم می خورد این است که گوگل به طور اتوماتیک سوژه ها و صحنه هایی که نشان داده شدن آن ها صلاح نیست را سانسور می کند و شما نباید نگران باشید، چون با یک درخواست ساده تصاویری که از خود، ماشین و یا محل زندگی تان ضبط شده است، پاک می شوند! البته این مطلب برای عزیزان ایرانی، فقط در حد یک نوشته است! پس زیاد جدی نگیرید! D:

## YouTube

یوتیوب برای این ایجاد شد تا مردم سرتاسر جهان بتوانند ایده ها و عقایدشان را از طریق رسانه با دیگر مردم به اشتراک بگذارند. اما گاهی اوقات ممکن است ترجیح دهید ویدئو هایتان را که نشان دهنده ی ایده هایتان است، با یک گروه کوچک



از دوستان به اشتراک بگذارید. کار سختی نیست! تنها وقتی می خواهید ویدئویی را آپلود کنید، گزینه ی **unlisted** یا **private** را انتخاب کنید.

گوگل و رهنمود هایی درمورد حریم شخصی

Page | 41

خوب است تا با قابلیت های گوگل درباره حفاظت از حریم شخصی کاربران آشنا شوید! تاپیک بعدی را بخوانید.

## بهبود نتایج جستجو

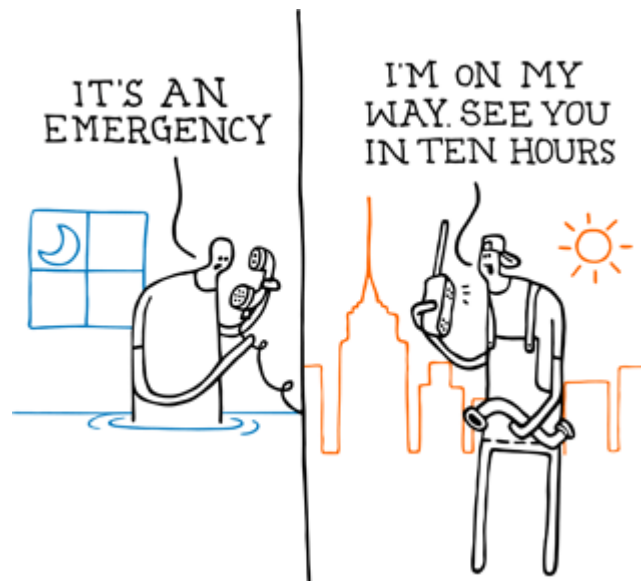
### بهبود کیفیت الگوریتم گوگل

تصور کنید برنامه ای ترتیب داده اید تا شام را بیرون میل کنید. در خیابان دو رستوران وجود دارد که باید از میان آن ها یکی را انتخاب کنید؛ یکی خلوت و دیگری شلوغ. مطمئناً رستوران شلوغ را انتخاب می کنید! همچنین، وقتی صحبت از "جستجوی گوگل" می شود، گوگل برای ارائه نتایج به جستجوی شما، از همین اصل استفاده می کند. یعنی برای این که بهترین نتایج از نظر مربوط بودن به منظور شما، ارائه شود، گوگل به الگوی میلیون ها کاربر دیگر در سرتاسر دنیا نگاه می کند و با یک جمع بندی، بهترین نتایج را به شما ارائه می کند. الگوریتم به این می گویند!

این کار با آنالیز کردن الگو ها توسط لاگ های اطلاعاتی ( [Logs Data](#) ) انجام می پذیرد که به دنبال آن، مهندسان گوگل قادر خواهند بود تا الگوریتم های جستجوی گوگل را بهبود ببخشند. اگر مهندسان متوجه شوند که کاربران برای هر جستار، بر روی اولین نتیجه ارائه شده کلیک می کنند، می فهمند که کارشان را خوب انجام داده اند، اما اگر کاربران گزینه " صفحه بعد " را کلیک کنند یا نحوه جستجویشان را تغییر دهند، آن ها متوجه می شوند که نتایج ارائه شده به کاربران مناسب نبوده و به فکر بهبود کیفیت الگوریتم خواهند افتاد.

## خصوصی سازی

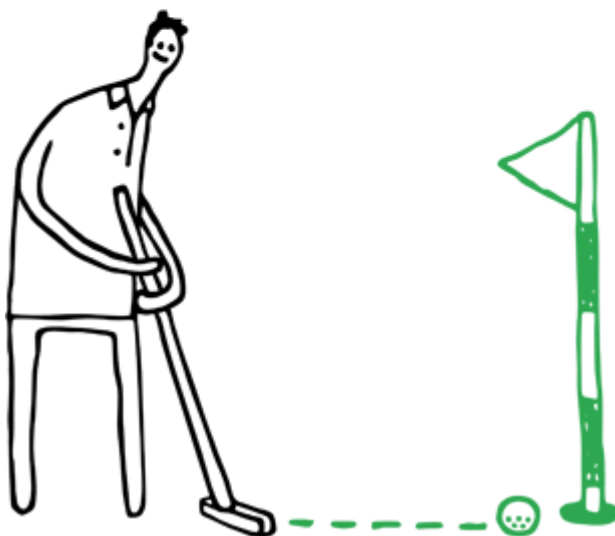
بیشتر کاربران در اکثر اوقات چیزی را که دنبال آن بوده اند، در گوگل پیدا می کنند، اما مطمئناً همیشه چنین اتفاقی نخواهد افتاد و دلیلش این است که گاهی پای حدس و گمان پیش خواهد آمد، مخصوصاً زمانی که مفهوم جستجو گنگ و مبهم باشد. مثلاً وقتی عبارت "Paris Hilton" را تایپ می کنید، منظور آن هتلی است که در پایتخت فرانسه است یا آن شخص مشهور؟! یا اگر "Chelsea" را تایپ می کنید، دبه دنبال اطلاعاتی راجب تیم چلسی هستید یا می خواهید راجب محله های مختلف لندن یا نیویورک تحقیق کنید؟! این ها سوالاتی است که گوگل با آن ها مواجه خواهد بود.



یک الگوریتم نمی تواند پاسخ تمامی این سوالات را در بر گیرد، به همین خاطر اگر گوگل کمی شما را بشناسد، اوضاع بهتر خواهد شد. یعنی اگر گوگل راجب ترجیحات و علاقه مندی های شما "سرنخ هایی" داشته باشد، نتایجی که در وهله اول به شما ارائه می شود، مناسب تر و در خور شما خواهد بود.

یکی از این سرنخ ها، موقعیت شما است. اگر در سان فرانسیسکو زندگی می کنید، مطمئناً به یک لوله کش نیویورکی زنگ نخواهید زد (حالا هزینه ی یک تماس که آن هم فقط بخاطر اعلام خطر است را تصور کنید)! به همین خاطر است که گوگل اغلب نتایجی را به شما ارائه می دهد که با موقعیت شما مطابقت دارد. یکی از روش های تعیین موقعیت که قبلاً به

آن اشاره کردیم، استفاده از IP است که به گوگل می گوید کامپیوتر شما تقریباً کجاست. در نتیجه، مجبور نخواهید بود برای پیدا کردن یک لوله کش، دور دنیا را بگردید!



دیگر سر نخ در میان جستجوهای قبلی شما است. اگر "Golf" را جستجو می کنید، منظورتان ماشین گلف است یا بازی گلف؟ فهمیدنش برای گوگل سخت است و نمی شود تنها با تکیه بر الگو دیگر کاربران، منظور شما را فهمید؛ پس باید کمی ریز تر شود! اگر در گذشته برای وسایل گلف در گوگل جستجو کرده اید، گوگل می تواند حدس بزند که منظور شما بازی

گلف است و نه ماشین گلف. اصولاً گوگل این را در طول چندین ساعتی که از گوگل استفاده می کرده اید می فهمد و مثلاً اگر دیروز برای باشگاه ها سرچ کرده اید و امروز برای گلف، ممکن است نتواند حدس بزند که منظور شما چیست.

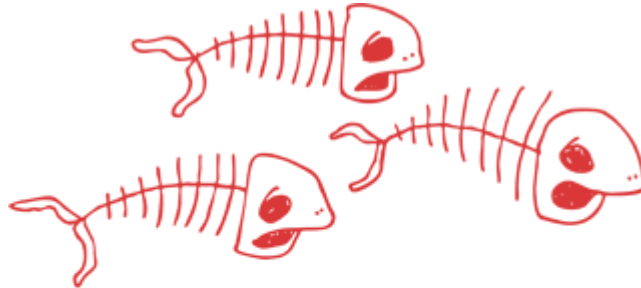
اگرچه شما به حساب گوگل خود وارد شوید و از Web History هم استفاده کنید، میزان خصوصی سازی حساب شما افزایش پیدا خواهد کرد و جستجو های شما با مفهومی که گوگل از آن ها استنباط می کند، مطابقت بیشتری پیدا خواهد کرد.

خوب است بدانید که اطلاعات چگونه سبب مناسب تر شدن نتایج جستجوی گوگل می شوند...

### افزایش امنیت سرویس های گوگل

باید به این نکته توجه داشت که نمی توان گفت هر کسی که در وب فعالیت می کند، تمایلات و اهداف خوبی دارد. شناسایی این بازیگران زیر پوستی و خراب کار، امنیت شبکه و کاربران را افزایش می دهد و استفاده از اطلاعات جستجو، برای این جور موقعیت ها به درد می خورد! آنالیز تک تک الگو های جستجو، به گوگل این امکان را می دهد تا بهتر بتواند بین ترافیک طبیعی و مفید وب و ترافیک مضر که توسط هکر ها به راه می افتد و به دنبال آسیب پذیری های امنیتی است، تمایز قائل شود. در ترافیک مضر، خرابکاران ممکن است برای دستکاری رنگینگ جستجو ی گوگل اقدام کنند و یا به طور اشتباه بر روی تبلیغات کلیک کنند که نتیجه اش، هزینه ی گزاف و ناعادلانه برای مبلغ خواهد بود. وقتی گوگل می خواهد بین الگو ها و رفتار های سالم و نرمال و ترافیک مضر تمایز قایل شود، در اختیار داشتن اطلاعات قدیمی می تواند معیار خوبی باشد و کمک شایانی بکند.

## افزایش سرعت جستجو

DID YOU *REALLY*  
MEAN **USED CARPS**?

تا حالا به این فکر افتاده اید که گوگل چگونه وقتی کلمه ای را اشتباه تایپ می کنید و یا حتی قبل از تایپ کردن کامل متن، کلمه درست ( منظور شما ) را حدس می زند؟! خوب این نتیجه ی سال ها مطالعه بر روی رفتار های مردم در وب است که این یادگیری ها به گوگل کمک می کنند تا پروسه جستجو در گوگل را سرعت ببخشد.

برای مثال، گوگل به این پی برده است که اکثر کاربران وقتی [flowres] را در محل جستجو ی گوگل تایپ می کنند، بلافاصله آن را تصحیح و [flowers] را تایپ می کنند. بنابراین گوگل پیش دستی می کند و اشتباه تایپی را می گیرد و عبارت صحیح را پیشنهاد می دهد. شایان ذکر است که گوگل برای تصحیح دیگر اشتباهات تایپی و پیشنهاد برای جستجو های مشابه، از یک اصل کلی استفاده می کند.

# JACK AND

— — — —

قابلیت [Autocomplete](#) نحوه جستجو ی میلیون ها کاربر را در روز بررسی می کند و با توجه به آن ها، وقتی شما در حال تایپ کردن عبارت مورد نظر خود هستید، کامل شده ی آن را در چندین روش مختلف به شما پیشنهاد می کند. مثلاً وقتی شروع به تایپ `[new york]` و یا حتی `[new y]` می کنید، بلافاصله پیشنهادهای مانند `New York Times.city` و `New York University` پدیدار می شوند که می توانید آن ها را انتخاب کنید.

برای این که عملیات جستجو از این هم سریع تر شود، گوگل، [Google Instant](#) را ارائه داد و وقتی که در حال تایپ کردن هستید، نتایج را به شما نشان می دهد! گمانه زنی ها حاکی از این است که این کار، باعث ذخیره ی ۲ تا ۵ ثانیه در هر جستجو خواهد شد. قبلاً، وقتی نتیجه ای را انتخاب می کردید، باید روی آن کلیک می کردید و منتظر می ماندید تا صفحه لود شود، اما حالا با این قابلیت ( `Instant pages` ) ، وقتی که می خواهید لینکی را برای کلیک کردن انتخاب کنید، برترین نتایج جستجو را در پس زمینه به شما ارائه خواهد داد که همین کار باعث صرفه جویی ۲ تا ۵ ثانیه ای در وقت می شود.

خوب است بدانید که گوگل چگونه از اطلاعات به منظور سرعت بخشیدن به عملیات جستجو استفاده می کند. تایپیک بعدی را بخوانید!

## کمک به جامعه

اطلاعاتی که گوگل از نحوه ی جستجوی مردم به دست می آورد، تنها به گوگل کمک نمی کند، بلکه می تواند برای تمام جوامع سر تاسر دنیا مفید باشد.

## بیماری ها

تصور کنید در محلی دور افتاده مردی در گوگل کلمه [ تب ] را تایپ می کند و چند دقیقه بعد و در همان اطراف، فرد دیگری عبارت [ درد ماهیچه ] را جستجو می کند و به همین ترتیب بر جمع افرادی که عبارات مشابهی را از یک منطقه مشابه جستجو می کنند، افزوده می شود. این جاست که متوجه می شویم آن جا خبری است!

Page | 47

گاهی اوقات الگو های کلی جستار ها، نزدیک به واقعیت هایی هستند که در دنیای واقعی در حال اتفاق افتادن است. وقتی این وجه اشتراک قوی تر است، با یک جستجوی ساده در نت می توان خیلی سریع تر و آسان تر نسبت به جستجو در دنیای واقعی، از وقایع با خبر شد. بنابراین با گردآوری و استفاده از اطلاعات جستجوی میلیون ها کاربر، می توان از اتفاقات ناگوار پیشگیری کرد و به حرفه ای ها وقت بیشتری اختصاص داد تا بهتر بتوانند نتیجه گیری کنند.

در سال ۲۰۰۸، گوگل متوجه شد نتایج بدست آمده از جستار ها، نشانه های خوبی از شیوع آنفولانزا هستند. آن طور که به نظر می رسید، یک یا دو هفته طول می کشید تا سیستم های مراقبت و اعلام بحران این بیماری، دست بکار شوند و به طور عمومی ماجرا را شفاف سازی کنند. اما جستار های گوگل خیلی سریع تر و بهتر از این هستند! با فعال سازی سیستم پیش بینی حوادث ( آنفولانزا)، Google Flu trends قادر است تا به سرعت در مورد این بیماری اعلام خطر کند. گوگل با استفاده از بینشی مشابه، در مورد بیماری های دیگر نیز دست به کار شده است و برای "تب" هم سیستم اعلام خطر راه اندازی کرده است.

شایان ذکر است که Google Flu Trends به هیچ وجه برای شناسایی افراد مورد استفاده قرار نمی گیرد و تنها اطلاعات هفتگی جستار ها را گردآوری می کند. گوگل همچنین به میلیون ها جستار کاربران در سرتاسر وب تکیه می کند و اطلاعات و الگو هایی که به دست می آید، نتایجی کلی هستند و بر طیف گسترده ای از کاربران دلالت دارند.

## اقتصاد

با مطالعه بر روی جستار های مردم، گوگل به اتفاقات دیگری نیز پی می برد که از مثال آن ها می توان به تغییرات وضعیت اقتصادی اشاره کرد. برای مثال، بانک انگلیس ، روند های جستجو ی مربوط به مشتری های بریتانیا را دنبال می کند. با بررسی دقیق تغییرات در درخواست کالا و تورم، بانک تمایل خواهد داشت تا گزارش های اقتصادی سریع تر منتشر شوند و در نتیجه تصمیمات اقتصادی بهتر و سریع تر گرفته شوند.

## Google Correlate

گوگل می داند که اطلاعات بیشماری را می توان از بررسی جستار ها به دست آورد و به همین خاطر، [Google](#) [Correlate](#) را معرفی کرد. این به محققان این اجازه را می دهد تا لیستی از جستار ها را که با وقایع دنیای واقعی مطابقت بیشتری دارند، در اختیار داشته باشند.

خوب است بدانید که چطور اطلاعات جستار ها به گوگل این امکان را می دهند تا به جامعه کمک کنیم، تاپیک عددی را بخوانید!



## اطلاعات خود را مدیریت کنید

اطلاعاتی که با گوگل و وب سایت ها به اشتراک می گذارید

Page | 49



گوگل همواره به این اعتقاد دارد که یکی از فاکتور هایی که برای شما بسیار مهم است، کنترل و مدیریت اطلاعات است. مطمئناً روش ها و ابزار های مختلفی وجود دارند تا به این مهم جامه ی عمل ببوشانند، اما در این تاییک قصد داریم به روش هایی بپردازیم که با استفاده از آن ها می توان بر اطلاعاتی که با گوگل و وب سایت های دیگر به اشتراک می گذارید، مدیریت داشت. گوگل کلکسیونی از ابزار های امنیتی حریم خصوصی را ارائه کرده است که قصد داریم در این بخش به مشهور ترین و بهترین های آن ها بپردازیم.

## چگونه کوکی ها را مدیریت کنیم

همان طور که گفته شد، هر وقت که مایل باشید، می توانید کوکی ها را از طریق تنظیمات مرورگر حذف کنید. همچنین می توانید آن ها را غیر فعال کنید، اما توجه داشته باشید که بیشتر وب سایت ها بدون وجود کوکی ها عملکرد خوبی نخواهند داشت؛ مثلاً قادر نخواهید بود تا کالایی را به سبد خرید اضافه نمایید و یا وارد حساب کاربری شوید. می توانید در مورد [پاک](#)

کردن کوکی ها، فعال کردن آن ها و مدیریت آن ها در مرورگر کروم اطلاعات بیشتری در Help Center گوگل پیدا کنید.

خوب است دانید که چگونه می توان کوکی ها را در وب مدیریت و یا حذف کرد. تاپیک بعدی را مطالعه کنید.

## داشبورد گوگل – Google Dashboard

اگر صاحب حساب کاربری گوگل هستید، [Google Dashboard](#) به شما کمک خواهد کرد تا جواب این سوال را پیدا کنید: "گوگل چه چیزهایی را در مورد من می داند؟" این سرویس اطلاعات نگهداری شده در حساب را به شما نشان می دهد و این قابلیت را به شما می دهد تا بتوانید تنظیمات حریم شخصی تان را در رابطه با تمام سرویس ها از یک محل کنترل کنید.

وقتی به داشبورد حساب خود وارد می شوید، با یک صفحه مواجه می شوید که در آن انواع سرویس هایی را که از آن ها استفاده می کنید و همچنین محتویات داخل آن را می توانید مشاهده کنید. این داشبورد می تواند به شما آمار بلاگ بلاگر، لیست مورد علاقه یوتیوب، عکس های آپلود شده و ... را دهد.

## Ads Preferences Manager

[Ads Preferences Manager](#)، به شما اجازه می دهد تا اطلاعاتی را که گوگل با استفاده از آن ها، تبلیغات مبتنی بر علاقه مندی را به شما نشان می دهد، مشاهده و یا ویرایش کنید.

علاقه مندی های شما بر روی یک کوکی تبلیغاتی که در مرورگر نگهداری می شود، ذخیره شده است. با استفاده از Ads Preferences Manager می توانید طبقه بندی کوکی را ویرایش کنید. برای مثال، اگر شما "golf" را به لیست علاقه مندی های خود اضافه کنید، تبلیغات بیشتری را در مورد golf خواهید دید. اما اگر از یک کامپیوتر دیگر و یا مرورگر دیگری استفاده کنید، طبقه بندی علاقه مندی های شما همراهتان نخواهد بود، چون آن طبقه بندی تنها مخصوص به کوکی مرورگر قبلی بود.

اگر هم مایل باشید، می توانید به کل این سرویس را غیر فعال نمایید؛ در نتیجه مانند گذشته تبلیغات متنوعی را خواهید دید که حتی ممکن است با علاقه مندی های شما هم جور در نیایند.

اگر بخواهید به طور کلی انصراف خود را از این قابلیت ( تبلیغات مبتنی بر علاقه مندی ) در تمام مشترکان کمپانی های NAI اعلام کنید، می توانید افزونه ی Keep My Opt-Outs را برای کروم دانلود نمایید.

اگر هم مایل نباشید تا این گونه تبلیغات را بر روی برنامه های موبایل و یا کلاینت هایی که از ID ناشناس استفاده می کنند ببینید، می توانید انصراف خود را با استفاده از قسمت [مدیریت مخصوص](#) اعلام کنید.

خوب است بدانید که می توانید از [Ads Preferences Manager](#) که شما اجازه می دهد تا اطلاعاتی را که گوگل با استفاده از آن ها ، تبلیغات مبتنی بر علاقه مندی را به شما نشان می دهد، مشاهده و یا ویرایش کنید، استفاده کنید. تاپیک بعدی را بخوانید.

## انتقال اطلاعات با فاکتور آزادی و امنیت!



گوگل معتقد است که این حق شماست که هر وقت خواستید، اطلاعاتتان را از محصولات (سرویس ها) گوگل انتقال دهید. این شرکت یک تیم مهندسی مخصوص به نام [Data Liberation Front](#) دارد و هدفش این است که پروسه انتقال اطلاعات از محصولات گوگل و همچنین به آن ها را آسان تر سازد.

با وجود این، می توانید یک نسخه کپی از اطلاعاتتان را در کامپیوترتان نگهداری نمایید و یا اگر قصد مهاجرت به محصول دیگری را دارید، اطلاعاتتان را از محصول گوگل به آن انتقال دهید. گوگل یک تیم آزادی اطلاعات به نام [Google Takeout](#) ایجاد کرده است که پروسه انتقال اطلاعات از محصولات گوگل و همچنین به آن ها را آسان تر می سازد.

## خصوصی سازی جستجو

گاهی اوقات گوگل، نتیجه جستجوی شما را بر اساس سابقه فعالیت های قبلی که در گوگل داشتید، خصوصی سازی می کند؛ فعالیت هایی که شامل انجام دادن یک جستجو در گوگل و کلیک کردن بر روی نتایج آن جستجو است. نحوه این کار بستگی به این دارد که واد حساب گوگل خود شده باشید و یا نشده باشید. بنابراین اگر می خواهید این قابلیت را غیر فعال کنید، دستور العمل ها کمی در این مورد فرق خواهند کرد.

جستجوگر هایی که لاگین کرده اند:

برای غیر فعال کردن این قابلیت، تنها باید [Web History](#) را از حساب خود حذف کنید. نحوه حذف هم به این شکل است که هم می توانید آن را به طور کلی غیر فعال کنید و هم می توانید به طور تک تک به حذف آیتم ها بپردازید. توجه داشته باشید که با حذف این سرویس، تمام جستجو های قبلی شما را از تاریخچه وب حذف می شوند.

جستجو گر هایی که لاگین نکرده اند:

اگر به حساب گوگل خود وارد نشده اید، گوگل جستجو های شما را بر اساس تاریخچه جستجو های شما که در [کوکیمرورگر](#) تان ذخیره شده است، خصوصی سازی می کند. شما هم می توانید [این سرویس را غیر فعال نمایید](#) و یا با [پاک کردن کوکی های مرورگر](#)، راه ساده تری را برای این کار انتخاب کرده باشید!

خوب است بدانید که می توانید نحوه خصوصی شدن نتایج جستجو را خودتان انتخاب کنید. تایپیک بعدی را بخوانید.

Google Talk

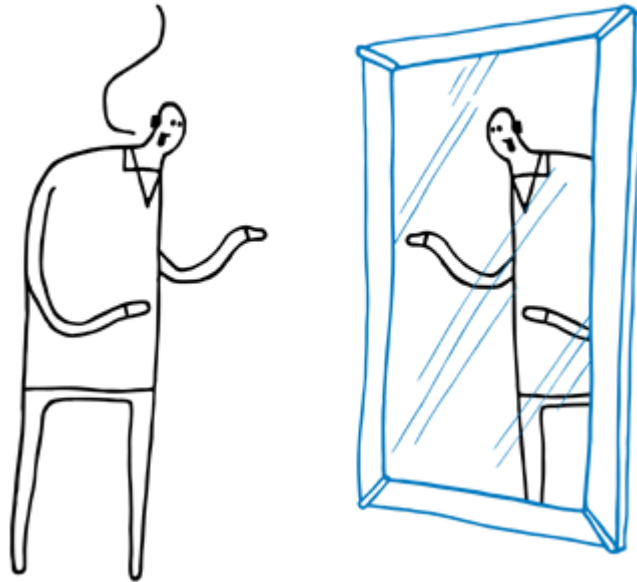
Page | 54



گوگل تاک، سرویس چت جی میل و دیگر محصولات گوگل، به شما این اجازه را می دهد تا از خلط شدن محتویات چت جلوگیری کنید. این گونه چت ها، در تاریخچه چت جیمیل شما ذخیره نخواهند شد. وقتی یک چت را به این حالت در می آورید، شما و مخاطبتان پیغامی را دریافت خواهید کرد مبنی بر این که محتویات این چت ذخیره نخواهد شد، مگر این که یکی از شما دو نفر تنظیمات را تغییر دهد.

## "من" در وب

FASCINATING



مدیریت بر روی اطلاعاتی که به اشتراک می گذارید، شبیه به دعوت از چند نفر برای صرف شام است؛ شما آن ها را در اطراف خانه می گردانید؛ غذای خوشمزه ای درست می کنید؛ اما آن ها فقط چیزهایی را می بینند که شما دوست دارید ببینند، چون احتمالاً دوست ندارید تا آن ها همه چیز ها را ببینند و ممکن است بعضی چیز ها را مخفی نمایید. این قضیه در مورد وب هم صدق می کند: شما اطلاعاتی را از خودتان به اشتراک می گذارید، اما دوست ندارید تا مردم از همه اطلاعات شما با خبر شوند.

اولین قدم مهم در کنترل کردن اطلاعاتی که مردم در وب قادر به مشاهده آن ها هستند، این است که بدانید چه چیز هایی از شما در وب منتشر شده است. هویت آنلاین شما تنها بر اساس چیزهایی که پست می کنید مشخص نمی گردد، بلکه پست های دیگران نیز - یک نظر در بلاگ شما، تگ عکس و یا پاسخ به نوشته نمایه (Status post) - در مورد شما بر هویت شما تاثیر می گذارند. وقتی کسی اسم شما را در یک موتور جستجو مانند گوگل جستجو می کند، نتایجی که بدست

می آیند تلفیقی خواهد بود از اطلاعاتی که خودتان پست کرده اید به علاوه اطلاعاتی که دیگران در مورد شما منتشر کرده اند.

سرویس گوگل، [Me on the Web](#) ، به شما در امر کنترل هویت آنلاین تان کمک می کند. یکی از این کمک ها، تنظیم نمودن [Google Alerts](#) است که بر اساس آن، هنگامی که اسم شما در یک وب سایت و یا داستان های خبری ذکر می شود، پیغام دریافت خواهید کرد. این سرویس همچنین به طور اتوماتیک چند فاکتور جستجو را که ممکن است برایتان مهم باشد، پیشنهاد می دهد.

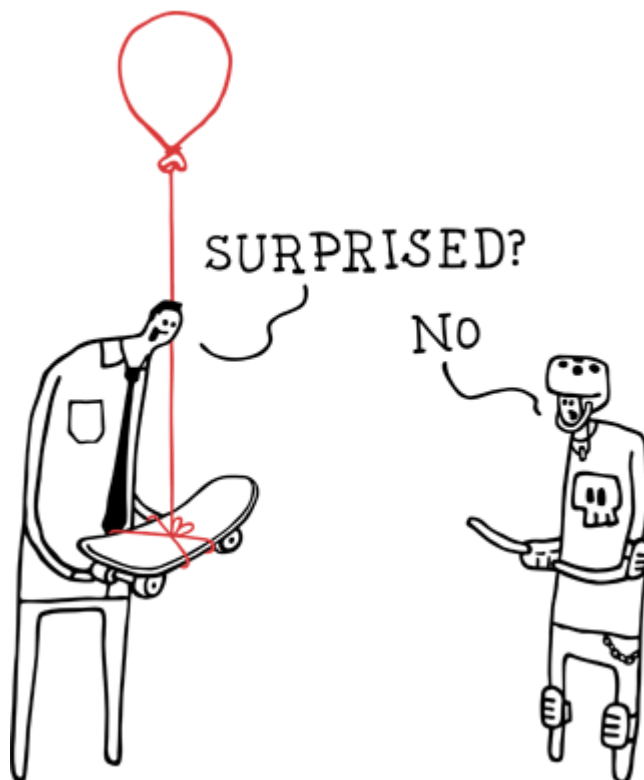
این قابلیت همچنین لینک هایی به منبع هایی که اطلاعاتی را در مورد کنترل اطلاعاتی که از شما در وب پست می شود، شامل می شوند، ارائه می دهد. این اطلاعات شامل نکاتی در مورد برقراری ارتباط به وب مستر یک سایت و درخواست برای حذف کردن اطلاعات و یا اضافه کردن اطلاعاتی توسط خودتان برای کاهش رابطه اطلاعاتتان با وب سایت ها خواهد بود.

شما می توانید این قابلیت را که زیرمجموعه ای از [Google Dashboard](#) است، در زیر Account details پیدا کنید.



## حالت Incognito در کروم

Page | 57



تصور کنید می‌خواستید هدیه‌ای را برای سورپرایز کردن شخصی به او بدهید. حتماً این‌ا هم می‌دانید که اگر آن شخص از هدیه‌بویی می‌برد، اسمش دیگر سورپرایز نمی‌بود. دلیل این‌هم که ممکن است ترجیح دهید روند مرور وب را ناشناسانه انجام دهید، همین است. گوگل کروم، مانند بسیاری از مرورگرها، قابلیت جستجوی ناشناس را ارائه داده است. این قابلیت در کروم با نام Incognito mode شناخته می‌شود. وقتی این حالت را انتخاب کنید، صفحاتی را که باز می‌کنید و یا فایل‌هایی را که دانلود می‌کنید در تاریخچه مرورگر ذخیره نخواهند شد. همچنین تمام کوکی‌های جدید در هنگام بستن پنجره حذف خواهند شد.

شایان ذکر است که بعضی اوقات، حتی در حالت Incognito، سایت‌ها اطلاعاتی را که در فرم‌هایشان وارد کرده بودید را به یاد می‌آورند. اگر هم سرویس دهنده‌ی اینترنت شما (ISP)، توسط شیطان فریب داده شود و آمار صفحاتی را که باز می‌کنید بدست آورد، دیگر ناشناس نخواهید بود!

## Google + و دکمه +۱

گوگل پلاس پروژه ای از سوی گوگل است که یک شبکه اجتماعی تلقی می شود و به کاربران، راه جدیدی را برای به اشتراک گذاری فایل ها ارائه کرده است؛ راهی که بس شبیه به روابط روزمره ی زندگی دنیا است. گوگل پلاس به شما این امکان را می دهد تا به جای اشتراک تمام اطلاعات با هر کسی، مطالب مختلفی را با اشخاص مختلف به اشتراک بگذارید.

شرکت گوگل، گوگل پلاس را با فاکتور مهم حریم خصوصی ایجاد کرد و همچنین با فراهم آوردن قابلیت های متنوعی، این امکان را به کاربران داد تا بتوانند مطالب را تنها با کسانی که دوست دارند به اشتراک بگذارند. برای اطلاعات بیشتر، می توانید [Google+ Privacy Guide](#) را مشاهده کنید.

دیگر قابلیت به اشتراک گذاری گوگل پلاس، دکمه +۱ است. اگر شما به اصطلاح مطلبی را +۱ کنید، این معنی را می دهد که شما آن مطلب، سایت و یا سرویس را پسندیده اید و تمایل دارید آن را به دیگران نیز پیشنهاد دهید. هر کسی در وب می تواند در هنگام جستجو در گوگل و یا مطالبی که آن ها را +۱ کرده اید، مشاهده کند چه چیزهایی را +۱ کرده اید. به همین دلیل، حتما فقط صفحاتی را +۱ کنید که به طور تمام و کمال از آن خوشتان آمده است، چون +۱ کردن یک صفحه، به معنی پیشنهاد دادن آن به همه دنیا است!

## Google Docs

Google Docs به شما امکان ایجاد و به اشتراک گذاری اسناد را به طور آنلاین می دهد. یکی از نکات مثبت این سرویس، این است که به چند شخص از موقعیت های مختلف این اجازه را می دهد تا به اتفاق بر روی یک سند کار کنند. اما [تنظیمات به اشتراک گذاری](#) این اطمینان را به شما می دهند که کنترل این که چه کسی بتواند اسناد شما را مشاهده و ویرایش کند را داشته باشید. در این سرویس، سه آپشن مختلف وجود دارد: شخصی، هر کسی با لینک و عمومی در وب. همه

اسناد در بدو ایجاد شدن، در حالت شخصی قرار می گیرند، مگر این که خودتان تنظیمات را تغییر دهید و یا این که مشتری [Google Apps](#) باشید.

درست مانند دنیای خودمان، باید این نکته را همواره به خاطر داشته باشید که کسانی که مطالبی را با آن ها به اشتراک می گذارید ممکن است آن اطلاعات را باز نشر (re-share) کنند. اگر شما به کسی اجازه تغییر تنظیمات دسترسی به اسنادتان را بدهید، ممکن است آن ها افراد بیشتری را برای مشاهده و ویرایش اسناد دعوت کنند.

## Latitude

Google Latitude که در نسخه های [دسکتاپ](#) و [موبایل](#) عرضه شده است، به شما این امکان را میدهد تا به راحتی موقعیت خودتان را با خانواده و دوستان به اشتراک بگذارید. شما می توانید تنظیمات حریم خصوصی را در Latitude تغییر دهید؛ بنابراین قادر خواهید بود تا جزئیات دلخواهی را با کسانی که مایل هستید، به اشتراک بگذارید. شما انتخاب می کنید که چه کسانی و در چه حدی از جزئیات می توانند موقعیت تان را ببینند و یا حتی می توانید در هر زمانی، نسبت به پنهان کردن موقعیت از دید خاص و یا عام اقدام نمایید.

[Google Location History](#) یک قابلیت دلخواه است که شما می توانید آن را برای حساب گوگلی که در آن Latitude را استفاده می کنید، فعال نمایید. تا وقتی که اقدام به فعال کردن آن نکنید، هیچ تاریخچه ای از موقعیت های شما در حساب ذخیره نخواهد شد. می توانید تاریخچه موقعیت تان را بر اساس موقعیت های قبلی و طیف زمانی و یا به طور کلی حذف نمایید و یا آن را غیر فعال کنید تا از آن زمان به بعد هیچ یک از موقعیت های شما در تاریخچه ذخیره نشود. اگر هم این قابلیت فعال است، به طور ماهیانه ایمیلی مبنی بر فعال بودن آن برای شما ارسال خواهد شد.