امن‌ترین پیام‌رسان‌های دنیا کدامند؟

۱. واتس اپ (whatsapp)

اپلیکیشن پیام‌رسان واتس اپ در سال ۲۰۱۶ میلادی، محبوب‌ترین و پرکاربردترین پیام‌رسان توسط کاربران در سراسر جهان شناخته شد. این پیام‌رسان همچنین با توجه به اینکه از سیستم رمزنگاری پیشرفته end-to-end encryption بهره می‌برد، از ضریب امنیتی بالایی برخوردار است بدین گونه که مکالمات و اطلاعات مبادله شده میان کاربران و مخاطبان به صورت کامل محافظت شده بوده و این طور که گزارش‌های منتشر شده عنوان می‌کنند، مکالمات و اطلاعات شخصی و خصوصی آنها از سوی نهادهای دیگر قابل رصد و ردگیری نخواهد بود.

شرکت فیس‌بوک با در اختیار گرفتن و تصاحب شرکت واتس‌اپ در سال ۲۰۱۴، ۱۹ میلیارد دلار کسب کرد و از آن زمان تاکنون نیز با معرفی و افزودن

قابلیت‌های جدید بدنبال جذب و حفظ طرفداران این پیام رسان محبوب بوده است.

۲. سیگنال (Signal)

این پیام‌رسان که در سال ۲۰۱۴ میلادی آغاز به کار کرد، توانست در این مدت زمان کوتاه فعالیتش، به ضریب امنیتی بالایی دست یابد، هرچند که محبوبیت و آوازه آن چندان به اندازه سایر اپلیکیشن‌های پیام رسان معروف در جهان نشده است، اما بسیاری از متخصصان امنیت سایبری استفاده از آن را به عنوان یک پیام‌رسان امن به کاربران پیشنهاد می‌دهند. شیوه رمزنگاری این پیام رسان از واتس اپ تبعیت کرده و هیچ اطلاعاتی در سرویس‌ها و سرورهای اپلیکیشن سیگنال ذخیره نمی‌شود.

۳. جی دیتا چت (G data secure chat)

اپلیکیشن پیام‌رسان جی دیتا چت که به تازگی عرضه شده و به صورت رایگان در دسترس عموم کاربران قرار گرفته است، نیز چندان از محبوبیت سایر اپلیکیشن های معروف و همچنین تعداد دفعات دانلود زیادی برخوردار نشده است.

۴. تلگرام (telegram)

اپلیکیشن پیام‌رسان تلگرام هم که در دو سال اخیر از محبوبیت و استقبال بی نظیری از سوی کاربران بهره‌مند شده است، از سرعت و امنیت بالایی برخوردار است و علاوه بر پروتکل های رمزنگاری پیشرفته از قابلیت دیگری همچون مکالمه محرمانه (secret chat) برخوردار است.

۵. سیراس (Ceerus)

یکی دیگر از سرویس‌های پیام رسان اندرویدی، سیراس (Ceerus) نام دارد که توسط یک استارتاپ انگلیسی مجهز به سیستم‌های SQR معرفی و عرضه شده است. این اپلیکیشن که به منظور حفاظت از اطلاعات خصوصی و شخصی کاربران، شرکت‌ها و سازمان‌های مختلف طراحی و عرضه شد، از کاربران یک حساب کاربری کامل تهیه می کند و از سیستم رمزنگاری پیشرفته بهره می برد.

۶. پرایویت (Pryvate)

این سرویس پیام‌رسان نیز که در سال ۲۰۱۵ میلادی طراحی شد و در دسترس عموم کاربران قرار گرفت، از تماس صوتی و ویدیویی و مکالمات رمزنگاری شده بهره می برد و به کاربران در سیستم‌های عامل مختلف، خدمات ارسال پیام را ارائه می‌دهد. این پیام رسان توسط تجار و شرکت های تجاری از استقبال بی نظیری مواجه شده است.

۷. فیس بوک مسنجر

پیام رسان فیس بوک مسنجر نیز از سیستم رمزنگاری پیشرفته end-to-end encryption و همچنین مکالمات محرمانه استفاده می کند و طبق گزارش های منتشر شده، کاربران فیس بوکی از این پیام رسان استقبال زیادی کرده اند.

منبع: بیتوته

آیا اندروید به آنتی‌ویروس نیاز دارد؟

از همان ابتدای ورود دو سیستم‌عامل اندروید و iOS به بازار، بحث امنیت جزء لاینفک رقابت میان این دو بوده است. اپل و طرفدارانش همیشه روی امنیت بالای آیفون در مقابل گوشی‌های اندروید مانور داده و بدافزارهای اندرویدی را به‌عنوان شاهد مثال آورده‌اند!

این امر سبب شده عده زیادی اندروید را به مثابه ویندوز به همراه ویروس‌های متعددش ببینند و این سیستم‌عامل وجه خودش را در زمینه امنیت در میان درصد قابل توجهی از کاربران از دست بدهد. بر این اساس، بسیاری این سوال در ذهنشان شکل گرفته که اندروید واقعا تا چه میزان امن است؟ آیا یک کاربر عادی اندروید باید نگران «ویروس» گرفتن گوشی یا تبلتش باشد و بنابراین به دنبال یک آنتی‌ویروس خوب؟

پاسخ سوالات مطرح شده بنا به گفته مسئولان ارشد اندروید، منفی است. کمی پیش از کنفرانس سالانه گوگل در اوایل امسال، ایدرین لودویگ (Adiran Ludwig) مسئول امنیت اندروید به خبرنگاران این‌طور گفته بود: «آیا من فکر می‌کنم کاربران عادی اندروید نیازی به نصب

آنتی‌ویروس دارند؟ قطعا خیر. من فکر نمی‌کنم بیش از ۹۹ درصد کاربران نفعی از یک اپ آنتی‌ویروس ببرند.» علاوه بر این، لودویگ معتقد است روی تهدیدات بدافزارهای اندروید زیادی تاکید شده است.

از سوی دیگر، شرکت‌های امنیتی و سازندگان اپ‌های آنتی‌ویروس برای اندروید چندان با این ادعا موافق نیستند. از نظر آنها ماجرا مانند بقال و ماست ترش می‌ماند و گوگل قاعدتا هیچ‌گاه به ایرادات فروشگاه پلی‌استور و اپ‌های مشکوک در آن اعتراف نخواهد کرد، اما اجازه دهید قضیه را کمی دقیق‌تر بررسی کنیم.

انواع ویروس‌های اندرویدی

در اصطلاح کامپیوتری، ویروس به‌طور ساده نوعی برنامه مخرب است که خودش را بین دستگاه‌های مختلف تکثیر کرده و گسترش می‌دهد. این نوع برنامه‌های مخرب سالیان سال کاربران ویندوز را آزار داده و می‌دهد. در مورد اندروید نیز با توجه به محبوبیت و توسعه فوق‌العاده آن، تهدیدات آن نیز رو به فراوانی گذاشته است. از نظر فنی نمی‌توان به بدافزارهای اندروید ویروس گفت، زیرا امکان تکثیر ندارند، با این وجود، این اصطلاح کماکان برای هر نوع بدافزاری به کار می‌رود.

در حالت کلی، بدافزارهای اندرویدی را می‌توان در پنج نوع تقسیم کرد: دسته اول، کپی‌کارها هستند یعنی نرم‌افزارهای تقلبی هم‌شکل و هم‌نام بازی‌ها و نرم‌افزارهای مشهور که کاربران به اشتباه آنها را نصب می‌کنند. این بدافزارها پس از نصب، ممکن است اقدام به جمع‌آوری و ارسال داده‌ها یا استفاده از تبلیغات اپ‌های دیگر به نفع خود کنند. نرم‌افزارهای کرک‌شده نیز می‌توانند در این دسته قرار بگیرند.

دسته دوم، باج‌افزارها هستند که با قفل کردن دستگاه، سعی در اجبار کاربر به پرداخت مبلغی برای آزادسازی آن دارند!

دسته سوم، بدافزارهای رباینده (Hijacking) هستند. این بدافزارها با روش‌های مختلف مانند تبلیغات و نوتیفیکشن‌های فراوان به نحوی کنترل گوشی را از دست کاربر درمی‌آورند تا او به ناچار روی سایت یا تبلیغی که اپ می‌خواهد کلیک کند و گوشی آلوده شود.

دسته آخر نیز بدافزارهای فیشینگ (Phishing) هستند که با شبیه‌سازی صفحه ورود سایت‌های معتبر یا پیام‌هایی چون «اینجا کلیک کنید تا باتری‌تان افزایش یابد!» کاربر را به سمت ورود اطلاعات یا دانلود نرم‌افزارهای آلوده پیش می‌برند.

منشأ بدافزارهای اندرویدی

اصلی‌ترین و مهم‌ترین دروازه ورود بدافزارهای اندروید، منابع غیرمعتبر توزیع نرم‌افزار هستند. سایت‌هایی که انواع و اقسام نرم‌افزارهای پولی را به‌صورت رایگان قرار می‌دهند، دانلود فایل نصبی یک نرم‌افزار (apk) از تلگرام و دیگر شبکه‌های اجتماعی، مارکت‌های عجیب و غریب چینی و غیرچینی و مسیرهایی از این دست.

البته این به آن معنا نیست که در دیگر مارکت‌ها و حتی خود پلی‌استور بدافزار وجود ندارد. درصد زیادی از هکرها و برنامه‌نویسان این بدافزارها، از ایرادات امنیتی استفاده کرده و نرم‌افزارهایشان را به اشکال مختلف وارد پلی‌استور می‌کنند. گوگل نیز به‌طور مستمر این نرم‌افزارهای مشکوک را حذف و حفره‌های امنیتی کشفشده را می‌بندد، اما این روند در هر حال به‌صورت یک بازی موش و گربه پیش می‌رود!

بالاخره آنتی‌ویروس نصب کنم یا نه؟

پیش از آن‌که به فکر نصب آنتی‌ویروس بیفتید، چند نکته امنیتی بسیار مهم وجود دارد که با رعایتشان در ردیف آن دسته کاربرانی قرار می‌گیرید که اصلا نیازی به آنتی‌ویروس نخواهند داشت. اولین نکته آن است که مسیر ورودی بدافزارها را ببندید و تمام نرم‌افزارها و به‌روزرسانی‌هایشان را از پلی‌استور یا مارکت‌های معتبر داخلی دانلود کنید. هرگز سراغ دانلود و نصب نرم‌افزار از منبعی که نمی‌شناسید، نروید!

هنگام نصب و استفاده از نرم‌افزارها هم حواستان به درخواست اجازه‌های آنها باشد. اگر دیدید نرم‌افزاری درخواستی خارج از کارکرد متعارفش دارد یا از نصب آن خودداری کنید یا در نسخه‌های بالاتر اندروید، این اجازه را به آن ندهید.

نکته دوم، به‌روزرسانی خود اندروید است. در هر نسخه جدید اندروید، حفره‌های امنیتی بسیاری رفع می‌شود که امنیت گوشی شما را بالاتر می‌برد. بنابراین در دانلود و نصب نسخه جدید سیستم‌عامل گوشی‌تان شک نکنید!

نکته سوم ارتباطی به خود بدافزارها پیدا نمی‌کند، اما در هر صورت لازم است همیشه از داده‌های روی تلفن همراه‌تان بک‌آپ بگیرید و تا حدامکان از نگهداری داده‌های حساس روی آن خودداری کنید تا اگر اتفاقی چه نرم‌افزاری و چه سخت‌افزاری افتاد، فهرست نگرانی‌هایتان شامل از بین رفتن یا دزدی اطلاعات خصوصی نباشد!

ICDL چیست ؟

در بیشتر کشورهای توسعه یافته و صاحب فناوری و در بعضی کشورهای در حال توسعه آموزش علوم کامپیوتری و فراگیری دانش - IT Information Technology جزو برنامه های اصلی مدارس ، دبیرستانها و دانشگاهها به شمار می آید . در ایران نیز برنامه توسعه و کاربردی فناوری ارتباطات و اطلاعات موسوم به (تکفا) مهمترین برنامه دولت در زمینه توسعه ، گسترش و کاربردی ساختن IT در کشور محسوب می شود .

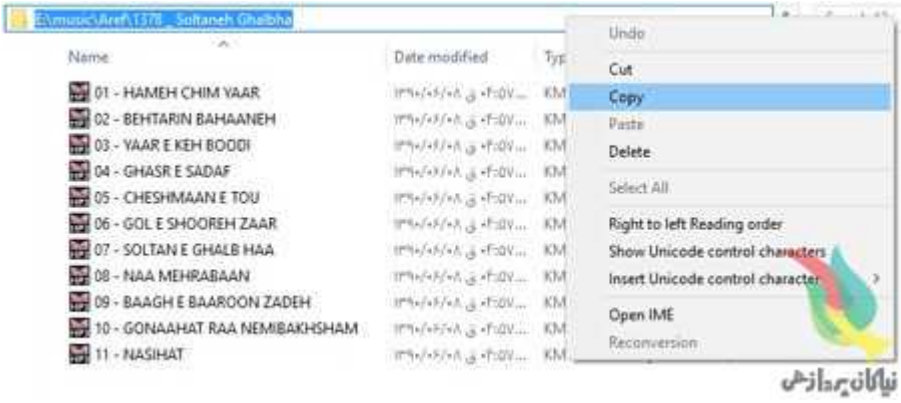
ICDL- International Computer Driving License ICDL گواهینامه ای است بین المللی جهت استفاده از کامپیوتر در حدی که نیازهای

مقدماتی و اصلی کاربر را پاسخگو باشد .

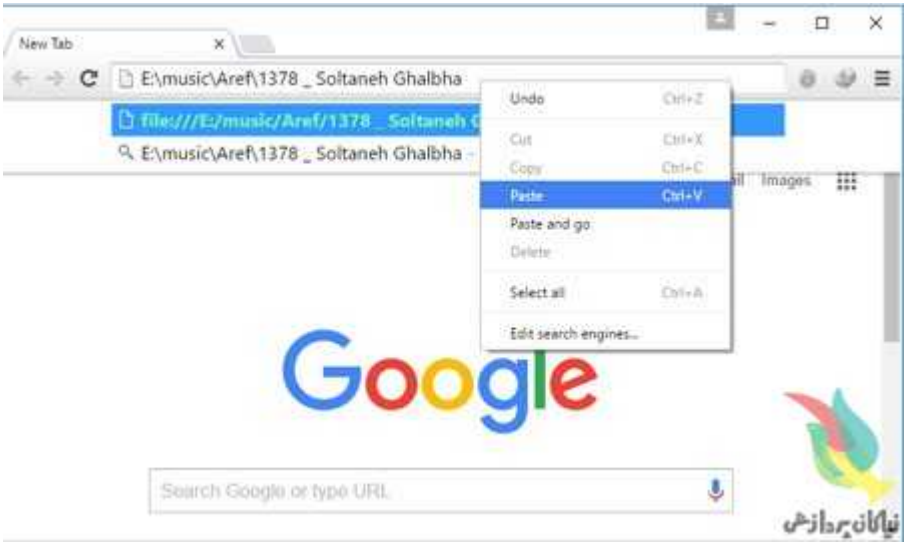
تغییر دسته‌جمعی نام فایل‌ها در محیط ویندوز به کمک اکسل

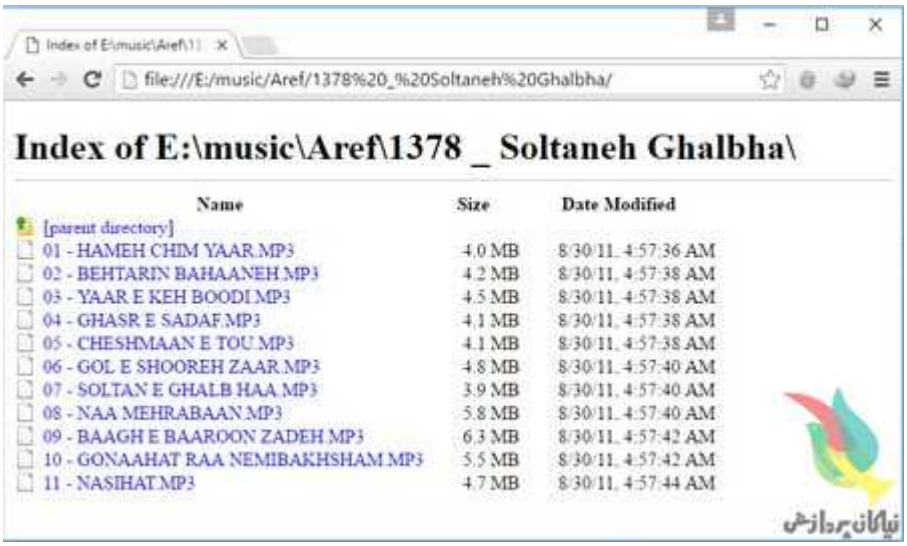
در این ترفند به نحوه‌ی تغییر دسته‌جمعی و یکجای نام فایل‌ها در محیط ویندوز به کمک نرم‌افزار مایکروسافت اکسل و Command Prompt خواهیم پرداخت. این روش از نام‌های فارسی نیز پشتیبانی می‌کند.

ابتدا وارد پوشه‌ای که فایل‌ها در آن قرار دارد شوید. سپس مسیر پوشه را Copy کنید.

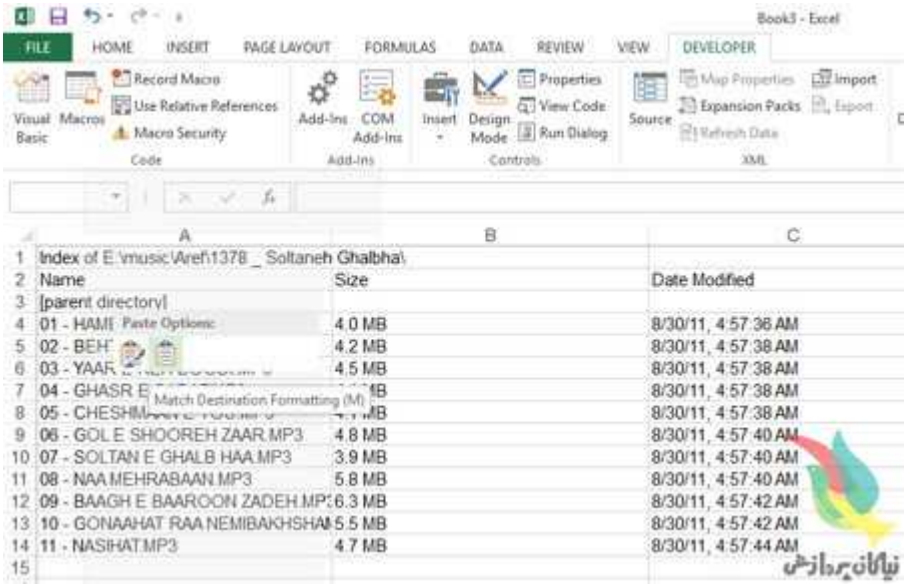


اکنون در مرورگر وب خود، در قسمت نوار آدرس این مسیر را Paste کرده و Enter بزنید.

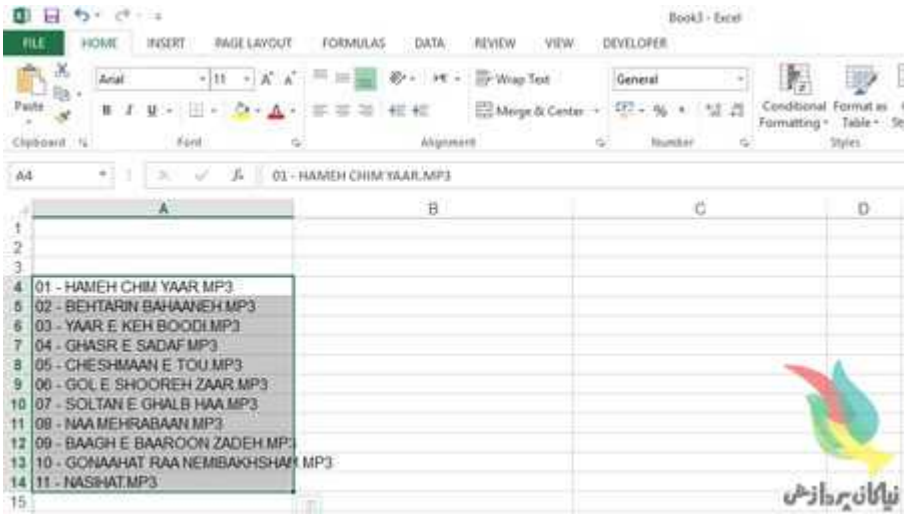




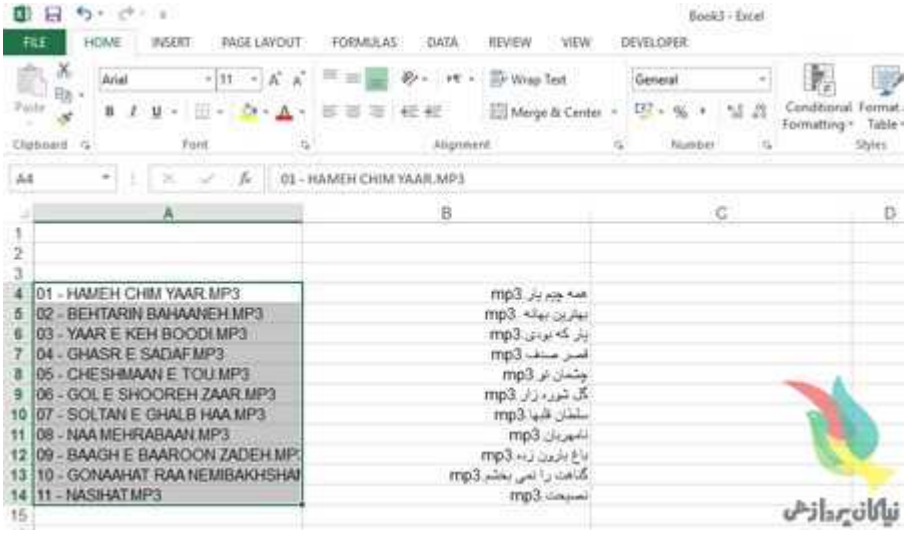
اکنون توسط کلیدهای ترکیبی Ctrl+A کل متون صفحه را انتخاب کرده و آن‌ها را Copy کنید. سپس داخل محیط اکسل در یک صفحه‌ی جدید، این محتوا را Paste نمایید.



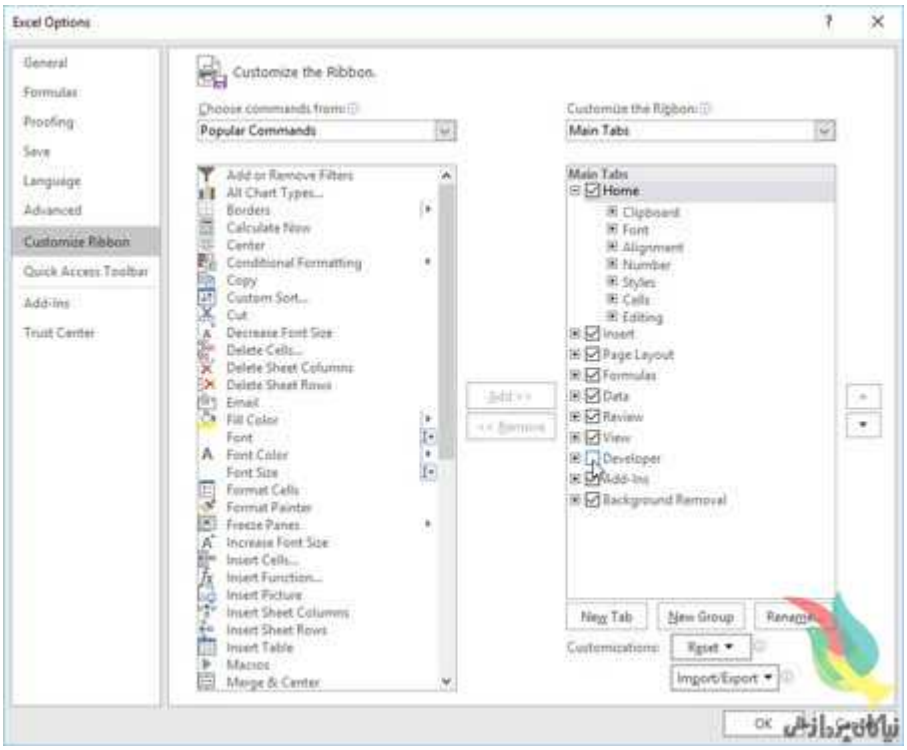
سلول‌های اضافی را پاک نمایید.



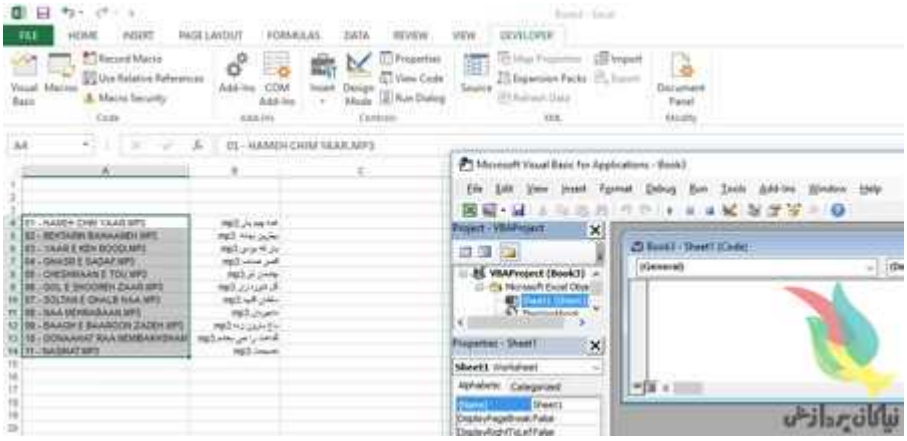
نام جدید با فرمتشان را در ستون مقابل بنویسید. سپس ستون نام قدیمی فایل‌ها را انتخاب کنید.



اکنون اگر تب Developer اکسل را تاکنون فعال نکرده‌اید، بر روی File و سپس Options کلیک کنید. سپس در تب Customize Ribbon، گزینه‌ی Developer را فعال کرده و روی OK کلیک کنید.

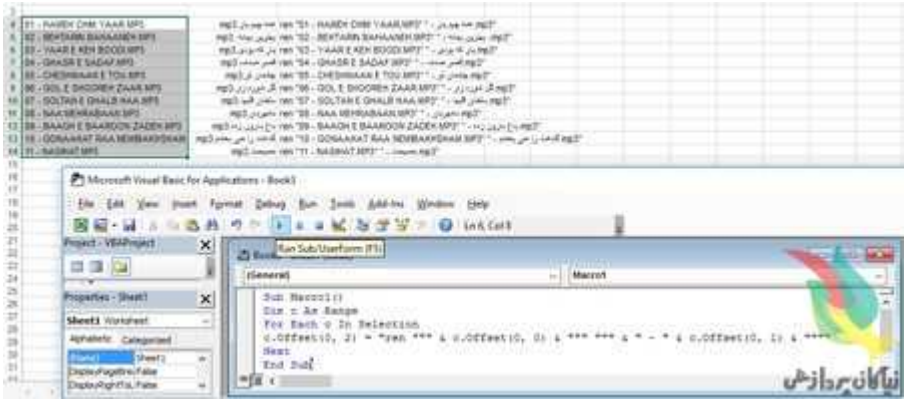


اکنون در محیط اکسل به تب Developer بروید و Visual Basic را انتخاب کنید (یا کلیدهای Alt+F11 را فشار دهید). سپس روی Sheet1(Sheet1) در سمت چپ دوبارکلیک کنید تا پنجره‌ی سفید رنگ برنامه‌نویسی باز شود.

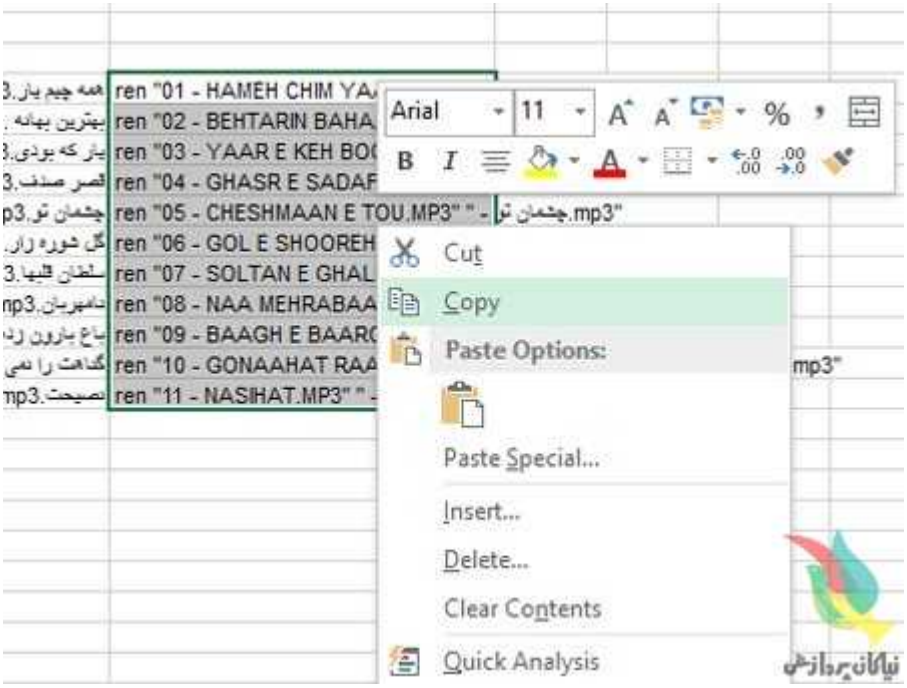


کد زیر را در کادر سفیدرنگ Paste نمایید:

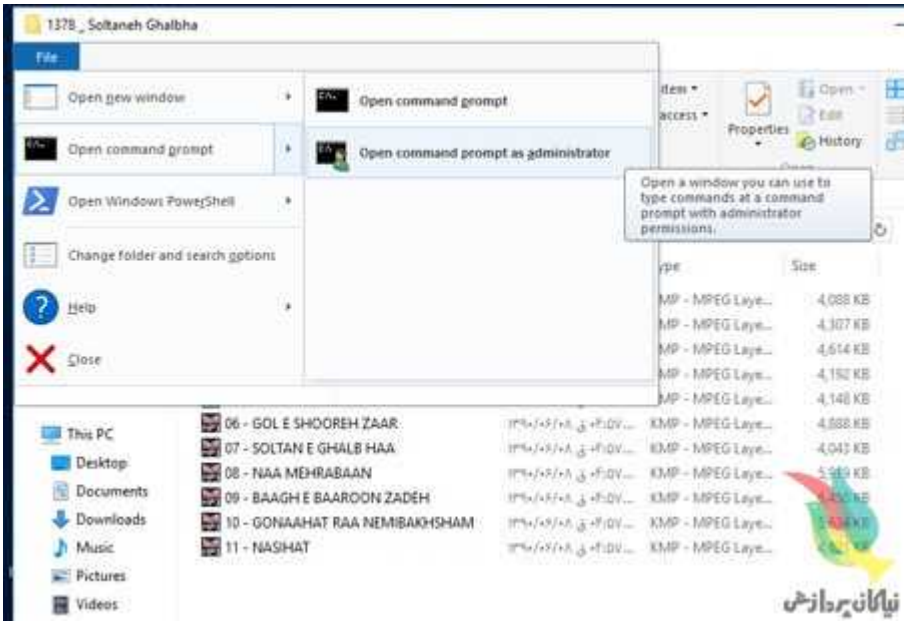
```
()Sub Macro1

Dim c As Range

For Each c In Selection

c.Offset(0, 2) = “ren “”” & c.Offset(0, 0) & “”” “”” & ” – ” &
”””“ & (c.Offset(0, 1

Next

End Sub
```



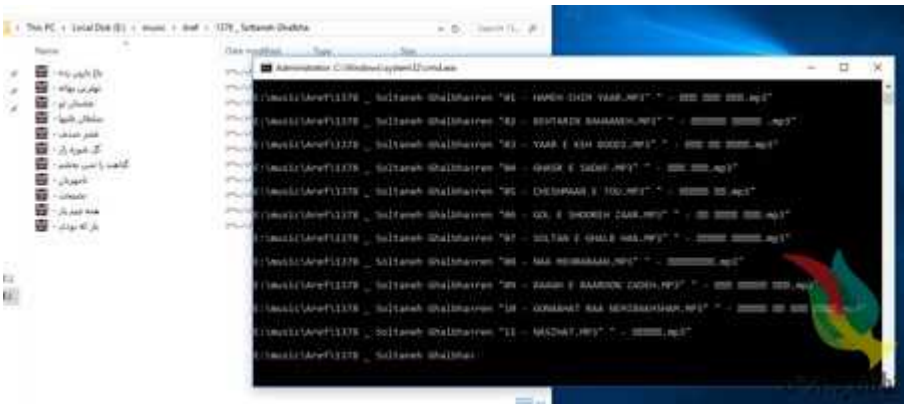
ستون ایجاد شده را Copy نمایید.



به پوشه‌ی مورد نظر بروید و Command Prompt را از منوی File باز کنید.



عملیات Paste را با فشردن کلیدهای Ctrl+V انجام دهید.



تغییر نام فایل‌ها انجام خواهد شد.

منبع: بیتوته

حملاتی که به گوشی های هوشمند انجام میشود

تشریح نفوذ به یک دستگاه تلفن همراه

چگونه یک هکر می‌تواند از گوشی شما سو استفاده کند؟

اندروید گوشی هوشمند شما ممکن است مبرا به نظر برسد، اما هنگامی که توسط بدافزارها مورد حمله قرار بگیرد متوجه می‌شوید که اطلاعات شما دیده و جعل می‌شود. شرکت در فعالیت های خودکار اینترنتی خطرناک است، و دزدیدن اطلاعات شخصی شما و حتی سرقت پول شما امکان دارد اتفاق بیافتد.

نظارت

- صدا
- دوربین
- لیست تماس
- موقعیت مکانی
- پیامک‌ها

جعل هویت

- فرستادن پیامک‌های شما
- ارسال پیام‌های ایمیل
- ارسال بر روی شبکه‌ی اجتماعی شما

سرقت اطلاعات

- اطلاعات حساب کاربری
- لیست ارتباطات
- لیست تماس‌ها
- شماره تلفن
- دزدیدن اطلاعات توسط برنامه‌های آسیب‌پذیر
- سرقت شماره سریال دستگاه (IMEI)

زیان مالی

- ارسال پیام نرخ حق بیمه
- دزدیدن شماره تراکنش احراز هویت (TANs)
- اخاذی توسط برنامه‌های مخرب
- شماره تلفن
- آنتی ویروس تقلبی
- برقراری تماس‌های گران‌قیمت

فعالیت‌های خودکار مخرب

- اجرای برنامه‌های هک
- تبلیغات مزاحم
- ارسال پیام نرخ حق بیمه

۳۵۰۰۰۰

۳۵۰،۰۰۰ ویروس اندرویدی توسط SophosLabs دیده شده‌است.

۵/۴$ میلیون

۵.۴ میلیون دلار هزینه متوسط نگهداری از یک شعبه اطلاعات در سال ۲۰۱۲ در امریکا بود.

۱۱۳

۱۱۳ گوشی هوشمند در امریکا در هر دقیقه گم می‌شود.

۹۹/۹۹$

هزینه ی عنوان شده توسط محافظان اندروید در برابر برنامه های مخرب.

مراقب اطلاعاتتان باشید!

با توجه به حملات سایبری هکرها در چند روز اخیر به سایت های دولتی و شرکت های بزرگ دنیا و حجم خسارات وارد شده به اطلاعات سازمان ها لازم است نکات زیر را رعایت نموده و راهکارهای پیشنهاد شده را با درجه اهمیت بالا انجام دهید:

حملات از نوع باج گیرها می باشند این نرم افزارها بدلیل ماهیت کاری که انجام می دهند از دید آنتی ویروس ها پنهان هستند و اطلاعات اسنادی(Word, Excel, Access, Powerpoint, PDF, E.Mail, SQL, Text) را رمزنگاری می کنند. فایل های رمزنگاری شده صرفا در قبال پرداخت مبالغ زیاد قابل استفاده می باشند و لازم به توضیح است که تاکنون هیچ روشی برای بازگشت و یا بازیابی داده های رمزنگاری شده وجود ندارد.

لازم است نکات پیشگیرانه زیر را مد نظر قرار دهید تا در دام این حملات گیر نیافتید:

۱ – از اطلاعات مهم کاری خود بر روی لوح فشرده CD یا DVD در زمان های متعدد پشتیبان تهیه کنید. توجه داشته باشید که لوح فشرده بعد از عمل رایت(Write) امکان آلوده شدن ندارد.

۲ – تحت هیچ شرایطی ایمیل های مشکوک را باز نکنید. ایمیل های مشکوک عموما با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا … می باشد. توجه داشته باشید اینگونه ایمیل ها عموما از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ – بر روی لینک های خبرهای مهیج مخصوصا در این بازه زمانی که با اخبار انتخابات نیز همراه می شود کلیک نکنید. برای مطالعه اخبار به سایت های معتبر خبرگزاری مراجعه کنید و از باز کردن لینک اخبار یا تصاویر و … در نرم افزارهای شبکه های اجتماعی خودداری کنید.

۴ – به هیچ عنوان از نرم افزارهای شبکه های اجتماعی بر روی سیستم های رایانه ای استفاده کنید. سعی کنید از نسخه های موبایلی آن شبکه ها استفاده کنید.

۵ – آنتی ویروس تان را بروز نگه دارید و از آنتی ویروس های کرک شده استفاده نکنید.

۶ – اگر دستگاه های ذخیره ساز مانند فلش یا هارد اکسترنال به سیستم خود متصل می کنید قبل از بازکردن آن ها را با آنتی ویروس اسکن کنید.

۷ – در صورتی که به باج گیر آلوده شدید(فایل های اسنادی شما به درستی باز نمی شوند و با پیامی مبنی بر رمز شدن اطلاعات مواجه شدید) بلافاصله کابل شبکه را از کامپیوتر خود جدا نمایید.

۸ – تاکید می شود حتما از داده های حساس خود بر روی لوح های CD و یا DVD فایل پشتیبان تهیه نمایید. همچنین می توانید با بهره گیری از نرم افزارهای فشرده سازی چون Winrar فایل های خود را فشرده نموده و ذخیره کنید.

تصویری گویا از علل حملات مهاجمان به گوشی ها

باج افزاری خطرناک با زبان فارسی

تایرنت «TYRANT» باج‌افزار جدیدی است که در روزهای اخیر به‌صورت متمرکز کاربران ایرانی را مورد هدف قرار داده است. این باج‌افزار فارسی براساس یک باج‌افزار متن باز ساخته و توسعه داده شده و اطلاعات کاربران در سیستم‌عامل‌های مایکروسافت ویندوز را برای باج‌خواهی رمزنگاری می‌کند.

? سازندگان تایرنت از بستر تلگرام با آدرس @Ttypern و ایمیل ناشناس rastakhiz@protonmail.com برای برقراری ارتباط با قربانی و بررسی پرداخت باج استفاده می‌کنند. این باج‌افزار فایل‌های متنی، تصاویر، ویدیویی و سایر فایل‌های حساس و مهم قربانی با پسوندهای ذکر شده در زیر را رمزنگاری کرده و سپس اقدام به مطالبه ۱۵ دلار باج به شکل ارز الکترونیکی از طریق سرویس Web Money می‌کند و تنها ۲۴ ساعت به قربانی خود مهلت می‌دهد تا مبلغ درخواست شده برای باج را بپردازد.

پسوند فایل‌هایی که تایرنت آن‌ها را رمزنگاری می‌کند:

aif, .apk, .arj, .asp, .bat, .bin, .cab, .cda, .cer, .cfg,. .cfm, .cpl, .css, .csv, .cur, .dat, .deb, .dmg, .dmp, .doc, .docx, .drv, .gif, .htm, .html, .icns, .iso, .jar, .jpeg, .jpg, .jsp, .log, .mid, .mp3, .mp4, .mpa, .odp, .ods, .odt, .ogg,.part, .pdf, .php, .pkg, .png, .ppt, .pptx, .psd, .rar, .rpm, .rss, .rtf, .sql, .svg, .tar.gz, .tex, .tif, .tiff, .toast, .txt, .vcd, .wav, .wks, .wma, .wpd, .wpl, .wps, .wsf, ..xlr, .xls, .xlsx, .zip

? مرکز ماهر ایران نیز با انتشار اطلاعیه‌ای در خصوص تایرنت اعلام کرده است که این باج‌افزار از طریق شبکه‌های اجتماعی با فریب دادن کاربران و تشویق آن‌ها به دریافت و اجرای فایل جعلی فیلترشکن سایفون، کاربران ایرانی را مورد هدف قرار داده و در حال انتشار است.

? بررسی‌های اولیه روی تایرنت نشان می‌هد که این باج‌افزار احتمالا نسخه اولیه و آزمایشی از یک حمله بزرگتر است. ضعف در پروسه رمزنگاری فایل‌ها و همچنین وجود برخی خطاها در تغییر تنظیمات ریجستری ویندوز و علاوه بر این، ساختن چندین نسخه آزمایشی مشابه دیگر توسط سازندگان این باج‌افزار، گواه این مساله است. همچنین خوشبختانه درصد قابل توجهی از آنتی‌ویروس‌ها در حال حاضر امکان شناسایی و حذف این باج‌افزار را دارند.

? باید توجه داشت که تایرنت با تکیه بر تکنیک‌های مهندسی اجتماعی قربانی می‌گیرد. استفاده از تکنیک‌هایی فریبنده برای ارائه محتوای آلوده و جعلی که می‌تواند برخی از کاربران را برای دریافت این باج‌افزار و اجرای آن در رایانه‌ها به خطر بیاندازد. برای مثال سازندگان این باج‌افزار پیش‌تر فایل‌هایی آلوده با عناوین فریبنده «khoosoosi shahla-96.EXE» و «pornwatch.EXE» را منتشر کرده‌اند و ماهیت حمله توزیع تایرنت نیز نشان می‌دهد که استفاده از دیگر روش‌های انتشار بدافزار و باج‌افزار، از جمله پیوست ایمیل و از طریق وب‌سایت‌های آلوده نیز امکان‌پذیر است.

حملات اخیر فعلا سیستم های کامپیوتری رو هدف قرار دادن ولی میتونن از طریق دستگاههای دیگه و گوشی های هوشمند و اینترنت و شبکه های مجازی پخش بشن.

این حملات غیرقابل جبران هستند و تمامی اطلاعات مهم سیستم کامپیوتری کد شده و غیرقابل استفاده خواهند شد.

از جمله: عکسها/موزیکها/ویدیوها/فایل های تایپی/نقشه ها/فایل های فشرده شده و هر اونچه که توسط شما یا افراد دیگه ذخیره شده باشه با یه کد مخرب بازنویسی میشن و تا کد بازکننده رو رو بهشون ندین باز نمیشن که این امر هم مسلما در ایران ممکن نبوده و نیست پس:

هر فایلی رو باز نکنین

هر ایمیل ناشناسی رو باز نکنین

به هر چت ناشناسی جواب ندین

عضو هر گروه و کانال ناشناس نشین

هر برنامه کامپیوتری رو از هر کسی قبول نکرده و نصب نکنین.

لطفا به عزیزان تون که در اینترنت گردی تجربه زیادی ندارن اطلاع بدین و بهشون تاکید کنین این حملات شوخی بردار نیستن.

اگر کسی از دوستان یا آشنایان درگیر چنین وضعی شد، حتما و به سرعت سیستم رو خاموش کنه و به هیچ وجه شخصا تلاشی نکنن. حتما سیستم شون رو برسونن به مراکز خدماتی با تجریه که جلوی ضرر بیشتر گرفته بشه و از روشن کردن دوباره سیستم قبل از پاکسازی خودداری کنن.

امیدوارم بتونیم با آگاهی رسانی به موقع از بروز خسارت به خودمون و دوستان مون جلوگیری کنیم.

لطفا آندرویدی ها از CM Security یا Lookout بهره ببرن.

آیفونی ها هم از LookOut یا McAfee یا هر برنامه امنیتی با برند جهانی استفاده کنن.

سیستم های کامپیوتری حتما برنامه امنیتی به روز و معتبر و دارای تاریخ اعتبار داشته باشند.

پیشنهاد من:

Symantec EndPoint Security

Kaspersky

Bitdefender

هست البته نه ویروس یاب اینها بلکه SYSTEM Security یا همون برنامه کامل امنیتی شامل ویروس یاب/ضد هک/ضد اسپم/ضد حملات شبکه ای که معمولا به اسم Total Security یا همون System Security معروف هستند.

از برنامه های دم دستی و تجاری مثل ESET یا Nodو مانند اینها کاری بر نمیاد.

چگونه از ریپورت اینستاگرام خارج شویم؟

معمولاً در شبکه‌های اجتماعی قوانینی وجود دارد که کاربران باید این قوانین را رعایت کنند. اینستاگرام نیز از این قاعده مستثنی نیست و قوانین و مقرراتی دارد که کاربران اینستاگرام موظف به رعایت این قوانین می‌باشند.

برای نمونه شما نمی‌توانید از تصاویر نژادپرستانه در پست‌های اینستاگرام خود استفاده کنید و یا پست‌های دیگران را به نام خود به اشتراک بگذارید! در سایت اینستاگرام در قسمت TERMS این قوانین بیان شده است. حال ریپورت اینستاگرام چیست؟

اگر کاربران قوانین اینستاگرام رعایت نکنند، این اقدام می‌تواند باعث حذف اکانت اینستاگرام آنها شود.

کاربران در اینستاگرام می‌توانند عمل خلاف قوانین دیگر کاربران را گزارش دهند، که به این عمل، ریپورت کردن گفته می‌شود. این ریپورت کردن می‌تواند شامل کاربر، پست، تصویر و یا کامنتی باشد. این موارد شامل ریپورت می شوند:

انتشار تصویر یا کامنت تبلیغاتی و اسپم

انتشار پست و تصاویر دیگران به نام خود

عدم رعایت قانون کپی رایت

انتشار تصاویر و کامنت‌های غیر اخلاقی

پست‌ها و کامنت‌هایی شامل خودکشی، تهدید و آزار و استفاده از مواد مخدر

این نکته را در نظر داشته باشید که اگر ریپورت‌های غیر واقعی ارسال شود، منجر به بسته شدن آن اکانت نمی‌شود.

رفع مشکل ریپورت اینستاگرام و بلاک شدن در اینستاگرام

در صورتی که برای کامنت گذاشتن، لایک کردن و فالو کردن و … با

مشکل مواجه شده‌اید، احتمالاً با مشکل ریپورت و بلاک شدن مواجه شده‌اید. بلاک شدن یک کاربر ممکن است توسط کاربران صورت گرفته باشد و یا توسط اینستاگرام کاربری بلاک شده باشد.

رفع ریپورت اینستاگرام و بلاک شدن توسط اینستاگرام

اگر برای کامنت گذاشتن در اینستاگرام با مشکل مواجه شده‌اید، احتمالاً در یک بازه زمانی بیش از حد مجاز کامنت ارسال کرده‌اید، این مشکل پس از چند ساعت رفع می‌شود. اما اگر با مشکل لایک کردن مواجه شده‌اید، در یک بازه زمانی بیش از اندازه لایک کرده‌اید.

بلاک شدن شما برای فالو کردن، به این معنی می‌باشد که شما یا در یک بازه زمانی بیش از اندازه فالو کرده‌اید و یا بیش از ۷۵۰۰ فالو کرده‌اید. رفع این نوع از بلاک شدن توسط اینستاگرام ممکن است تا یک ماه طول بکشد.

برای رفع مشکل بلاک شدن توسط اینستاگرام راهکارهای زیر را انجام دهید:

راهکار اول برای رفع بلاک شدن توسط اینستاگرام:

یکی از راهکارهای معمول، این است که از فالوورهای خود بخواهید تا برای شما کامنت انگلیسی ارسال کنند. در واقع با این روش به اینستاگرام ثابت می‌کنید که شما اسپم نیستید! به این منظور می‌توانید از تصاویر زیر به همراه یک پیام متنی استفاده کنید:

راهکار دوم برای رفع بلاک شدن توسط اینستاگرام:

راهکار دیگربرای رفع ریپورت اینستاگرام ، تغییر ایمیل اکانت می‌باشد. به این منظور وارد پروفایل خود شوید و گزینه Edit your profile را انتخاب نمایید. حال در قسمت Private information می‌توانید شماره تلفن و ایمیل خود را ویرایش کنید. بعد از تغییر ایمیل یا شماره تلفن، پیامی حاوی یک لینک ارسال می‌شود که باید بر روی آن کلیک کنید.

چگونه بفهمیم چه کاربری ما را ریپورت و بلاک کرده است؟

قبل از هرچیز باید متوجه شوید که چه کسی شما را بلاک کرده است، اما اینستاگرام اجازه نمی‌دهد شما به طور مستقیم چک کنید چه کسی شما را آنفالو و یا بلاک کرده است.

اگر دیگر نمی‌توانید پست‌های اکانت کاربری را مشاهده کنید، این احتمال وجود دارد که آن شخص شما را آنفالو و یا بلاک کرده باشد.

یکی از ترفندهایی که می‌توانید بفهمید چه کسی شما را بلاک کرده است، سرچ اکانت آن کاربر می‌باشد. به این منظور اگر به کاربری شک دارید که شما را بلاک کرده باشد، باید در صفحه جستجوی اینستاگرام، نام اکانت آن کاربر را وارد کنید، در صورتی که اسم او برای شما نمایش داده نمی‌شود، احتمالاً آن کاربر شما را بلاک کرده است.

اگر می‌توانید وارد صفحه اینستاگرام کاربر شوید اما وقتی او را فالو می‌کنید، جزء فالوورهای او نمی‌شوید و همچنان دکمه Follow را مشاهده می‌کنید، یعنی توسط او بلاک شده‌اید.

همچنین اگر دیگر اسم او جزء فالووینگ‌های شما نیست، بازهم می توان احتمال داد توسط آن کاربر آنفالو و یا بلاک شده‌اید.

همچنین اگر با اکانت جدید می‌توانید آن کاربر را فالو کنید ولی با اکانت فعلی خود نمی‌توانید، یعنی آن اکانت شما بلاک شده است.

لوگوی گوگل را به دلخواه تغییر نام دهید.

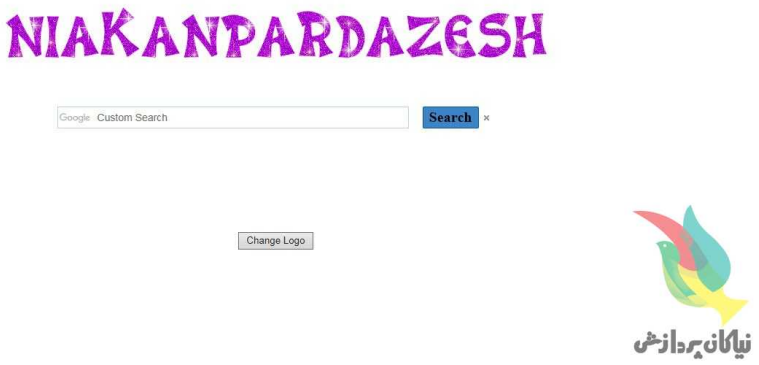
گوگل یکی از پرکاربردترین مرورگرها در بین کاربران وب است، یکی از قابلیت‌های این مرورگر تغییر نام آن به دلخواه شماست.

لوگوی گوگل را همیشه با رنگ های مختلف دیده اید و گاه به مناسبت‌های گوناگون اشکالی متفاوت از لوگوی گوگل برای شما به نمایش گذاشته شده است، ممکن است عده ای تغییر نام لوگوی گوگل را یک قابلیت جذاب و مناسب برای این مرورگر بدانند که می تواند در کنار تمامی قابلیت های گوگل، این مرورگر را در بین کاربران محبوب تر از گذشته کند.

تغییر نام لوگوی با یک ترفند ساده قابل انجام است و شما می توانید پس از انجام مراحل زیر هر بار که گوگل را باز می کنید به جای نام google، عنوانی را که انتخاب کرده اید، ببینید.

برای شروع در مرورگر گوگل عنوان goglogo را تایپ کنید و اینتر را بزنید.

سپس سایتی که به شما معرفی شده است را باز کنید. در قسمت your name کلیک کنید.

نام دلخواه خود را تایپ کرده و اینتر را بزنید.

همانطور که در تصویر زیر مشاهده می کنید صفحه گوگل به نامی که شما انتخاب کرده اید تغییر پیدا کرده است.