

امن‌ترین پیام‌رسان‌های دنیا کدامند؟



۱. واتس‌آپ (whatsapp)

اپلیکیشن پیام‌رسان واتس‌آپ 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 واتس‌آپ 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 اپلیکیشن‌های 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 پروتکل‌های 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 استارت‌آپ 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 می‌کند و از سیستم رمزنگاری پیشرفته بهره می‌برد.

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 می‌برد و به کاربران در سیستم‌های عامل مختلف، خدمات ارسال پیام را ارائه می‌دهد. این پیام رسان توسط تجار و شرکت‌های 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

ده مسنجر معتبر و امن دنیا !!!



پرینت گرفتن دو صفحه در یک صفحه در Word

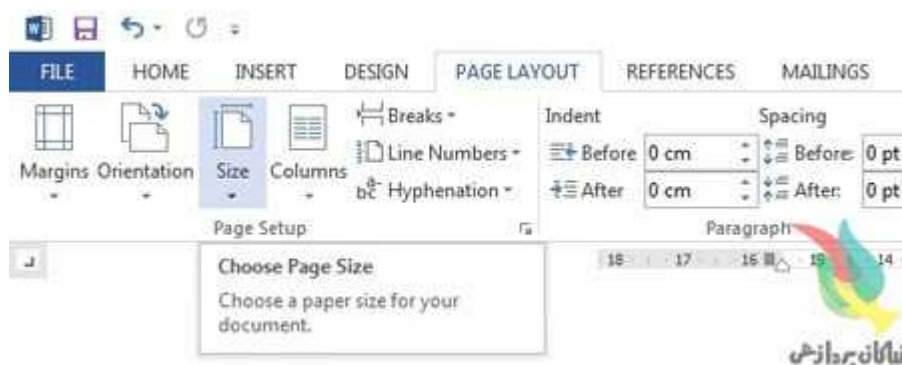


در زمان پرینت گرفتن برخی اسناد در ورد گاهی احتیاج پیدا می کنیم به علت کمبود کاغذ ، دو صفحه را در یک صفحه پرینت کنیم. یا زمان هایی پیش می آید که می خواهیم یک جزوه را در ابعاد کوچکتر چاپ کنیم. به عبارت دیگر در این مقاله خواهید آموخت که چگونه دو صفحه A5 را در یک صفحه A4 پرینت بگیرید.

” قبل از پرینت ، سایز کاغذ را به درستی انتخاب کنید. “

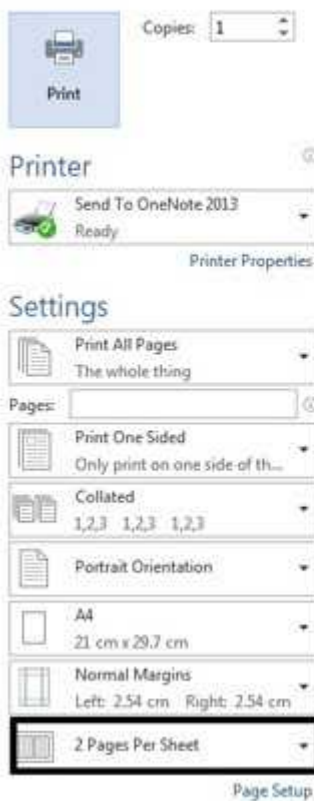
روش تنظیم کردن کاغذ و ابعاد پرینت

برای اینکه ابعاد پرینت شما به درستی تنظیم شود ابتدا فایل ورد خود را باز کنید و مطابق تصویر زیر ، ابعاد کاغذ را بر روی A4 تنظیم کنید. (وارد بخش Page Layout شوید و گزینه Size را بر روی A4 قرار دهید.) بعد از انجام این کار احتمال دارد تیتربندی ها و قسمت بندی های فایل شما کمی دچار تغییر شود که باید قبل از چاپ آنها را اصلاح کنید.



حال که نوع کاغذ را بر روی A4 تنظیم کردیم نوبت به پرینت گرفتن می‌رسد. پس از قرار دادن کاغذ در پرینتر مقدار مورد نیاز، دکمه های Ctrl+P را فشار دهید.

Print



2

1



نیکان‌مدانی

در پنجره پیش رو همان‌طور که در تصویر مشاهده می‌کنید مطابق با نسخه نرم افزار Word شما، گزینه ای برای تنظیم تعداد صفحه قابل چاپ در یک صفحه وجود دارد. این مورد به صورت پیش فرض بر روی ۱ Page Per Sheet می‌باشد. اکنون شما باید آن را بر روی گزینه ۲ Pages Per Sheet تنظیم کنید و در نهایت بر روی دکمه Print کلیک کنید.

در نسخه های قدیمی تر ورد، بعد از فشردن Ctrl+P بخشی به نام Zoom را پیدا کرده و گزینه Pages Per Sheet را بر روی ۲ تنظیم کنید.

آیا اندروید به آنتی‌ویروس نیاز دارد؟



از همان ابتدای ورود دو سیستم عامل 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 به عنوان شاهد مثال آورده‌اند!

این امر سبب شده عده زیادی اندروید را به مثابه ویندوز به همراه ویروس‌های متعددش ببینند و این سیستم عامل 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؟ قطعاً 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 آپ 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 اندرویدی، 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 بiftید، چند نکته امنیتی بسیار مهم وجود دارد که با رعایتشان در ردیف آن دسته کاربرانی قرار می‌گیرید که اصلاً 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 حد امکان 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!

مراقب اطلاعات‌تان باشید!



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

حملات از نوع باج‌گیرها می‌باشند این نرم‌افزارها بدلیل ماهیت کاری که انجام می‌دهند از دید آنتی‌ویروس‌ها پنهان هستند و اطلاعات اسنادی (Word, Excel, Access, Powerpoint, PDF, E.Mail, SQL, Text) را رمزنگاری می‌کنند. فایل‌های رمزنگاری شده صرفاً در قبال پرداخت مبالغ زیاد قابل استفاده می‌باشند و لازم به توضیح است که تاکنون هیچ روشی برای بازگشت و یا بازیابی داده‌های 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 عموماً با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا ... می باشد. توجه داشته باشید اینگونه ایمیل ها عموماً از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ - بر روی لینک های خبرهای مهیج مخصوصاً 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 نکنید. 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





چرا گوشی های تلفن همراه هدف مجرمان سایبری قرار می گیرند؟

✓ تلفن همراه شما، همه چیز را در مورد شما می داند.

اطلاعاتی نظیر: تصاویر خصوصی، اطلاعات شخصی و حساب های شبکه های اجتماعی، اطلاعات حساب بانکی و ... از جمله اهداف مجرمان سایبری اند.



✓ تلفن های همراه می دانند شما کجا هستید و کجا کار می کنید.

زمانی که از GPS گوشی خود استفاده می کنید امکان ردیابی موقعیت خود را فراهم کرده اید.



✓ تلفن همراه شما، مسیری به سمت کیف پولتان است.

استفاده از نرم افزار های بانکی در کنار مزایای خود می تواند به یکی از اهداف مجرمان سایبری تبدیل شود.



✓ تلفن های همراه به وسیله ای در شرکت ها و سازمان ها تبدیل شده است.

استفاده از تلفن های همراه در محل کار شرایطی را ایجاد کرده تا این ابزار به عنوان دروازه ای برای سرقت اطلاعات حساس سازمان ها محسوب شود.



نیایان پردازش

باج افزاری خطرناک با زبان فارسی



تایرنت «TYRANT» باج افزار جدیدی است که در روزهای اخیر به صورت متمرکز کاربران ایرانی را مورد هدف قرار داده است. این باج افزار فارسی براساس یک باج افزار متن باز ساخته و توسعه داده شده و اطلاعات کاربران در سیستم های مایکروسافت ویندوز را برای باج خواهی رمزنگاری می کند.

؟ سازندگان تایرنت از بستر تلگرام با آدرس Ttypern@ و ایمیل ناشناس rastakhiz@protonmail.com برای برقراری ارتباط با قربانی و بررسی پرداخت باج استفاده می کنند. این باج افزار فایل های متنی، تصاویر، ویدیویی و سایر فایل های 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 می کند و تنها ۲۴ ساعت به قربانی خود مهلت می دهد 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 می‌دهد 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 «khoodoosi 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 سیستم‌های کامپیوتری رو هدف قرار دادن ولی میتونن از طریق دستگاه‌های دیگه و گوشی‌های هوشمند و اینترنت و شبکه‌های 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 تجربه 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 Nod و مانند اینها کاری بر نمیاد.

چگونه از ریپورت اینستاگرام خارج شویم؟



معمولاً در شبکه های 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 می باشند.

چگونه از رپورت اینستاگرام خارج شویم؟



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 رپورت 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، رپورت کردن گفته می‌شود. این رپورت کردن می‌تواند شامل کاربر، پست، تصویر و یا کامنتی باشد. این موارد شامل رپورت می‌شوند:

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 رپورت‌های غیر واقعی ارسال شود، منجر به بسته شدن آن اکانت نمی‌شود.

رفع مشکل رپورت 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

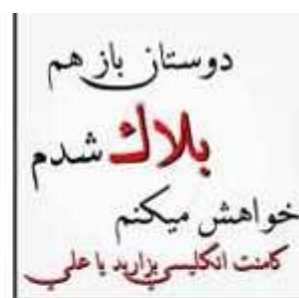
اگر برای کامنت گذاشتن در اینستاگرام با مشکل مواجه شده‌اید، احتمالاً در یک بازه زمانی بیش از حد مجاز کامنت ارسال کرده‌اید، این مشکل پس از چند ساعت رفع می‌شود. اما اگر با مشکل لایک کردن مواجه شده‌اید، در یک بازه زمانی بیش از اندازه لایک کرده‌اید.

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 دیگر برای 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 فالوینگ‌های شما نیست، بازهم می‌توان 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.

خاموش و روشن‌های مک



انجام برخی کارها در سیستم‌های عامل مختلف جزو امور عادی به‌شمار نمی‌رود، اما در برخی موارد ممکن است اطلاعات ارزشمندی را در اختیار شما قرار دهد.



یکی از این کارها، اطلاع یافتن از مدت زمانی است که رایانه شما روشن بوده یا بررسی تاریخچه زمان‌هایی که رایانه ریاستارت شده یا خاموش شده است. گرچه دانستن این اطلاعات برای یک کاربر عادی در شرایط طبیعی ضرورتی ندارد، اما همین اطلاعات در بررسی مشکلات رایانه یا رفع عیوب احتمالی مشاهده شده در آن می‌تواند بسیار موثر و ضروری باشد.

دوست دارید بدانید رمزگشایی جعبه سیاه رایانه در سیستم‌عامل مک چگونه است؟ با استفاده از این ترفند به روش‌های مختلفی می‌توانید به این اطلاعات دسترسی یابید:

روش اول (مدت روشن بودن رایانه)

در این روش از ابزار System Information کمک می‌گیریم. برای اجرای این ابزار از نوار منوی اصلی روی آیکون اپل کلیک کرده و کلید

Option را فشار دهید تا گزینه About This Mac به System Information تغییر کند سپس روی گزینه System Information کلیک کنید.

از ستون سمت چپ روی Software کلیک کرده و مدت زمان به نمایش درآمده (مدت روشن بودن رایانه در بوت فعلی) را در مقابل عبارت Time since boot در ستون سمت راست مشاهده کنید.

روش دوم (مدت روشن بودن رایانه)

ابزار ترمینال را اجرا کرده و فرمان uptime را در آن وارد کنید و کلید اینتر را فشار دهید.

با اجرای این فرمان، به ترتیب زمان فعلی رایانه، مدت زمان روشن بودن رایانه، تعداد پنجره‌های ترمینال در حال اجرا و میانگین پردازش‌های موجود روی سیستم‌عامل در بازه‌های زمانی ۱، ۵ و ۱۵ دقیقه اخیر به شما نمایش داده می‌شود.

روش سوم (تاریخچه ری‌استارت و خاموشی‌ها)

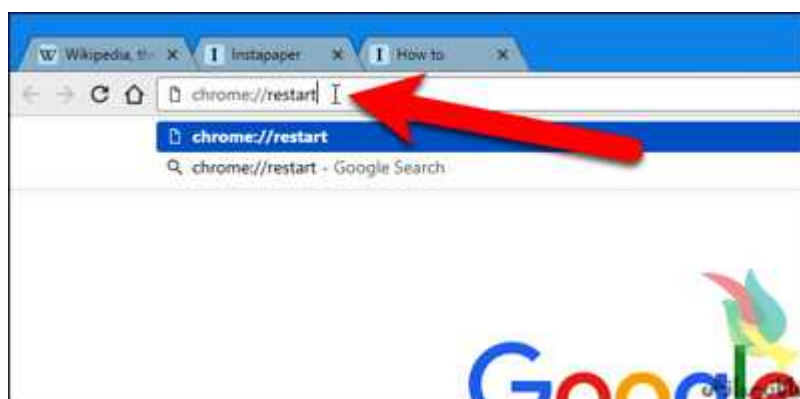
ترمینال را اجرا کرده و یکی از فرمان‌های last reboot یا last shutdown را در آن وارد کرده کلید اینتر را فشار دهید.

با اجرای هریک از این فرمان‌ها، تاریخچه کاملی از زمان کل ری‌استارت و خاموش شدن‌های رایانه در اختیار شما قرار می‌گیرد. این تاریخچه از ابتدای نصب سیستم‌عامل روی رایانه شما قابل مشاهده است و اگر می‌خواهید بدانید چند وقت پیش سیستم‌عامل رایانه را نصب کرده‌اید کافی است آخرین ردیف موجود را مشاهده کنید.

ری‌استارت کروم با میا نبر



در شرایط عادی مطمئناً نیازی به ریاستارت کردن مرورگر (بستن و اجرای مجدد آن) وجود ندارد، اما گاهی ممکن است به هر دلیلی چاره‌ای جز این کار نداشته باشید.



رایج‌ترین روش برای ریاستارت کردن مرورگر، استفاده از گزینه Close برای بستن آن و در ادامه اجرای مجدد با دوبار کلیک روی آیکون برنامه است. این روش مشکلی ندارد، اما همان‌طور که میدانید این صفحه به دوستان ترفند اختصاص دارد و مرورگر کروم نیز مملو از قابلیت‌های پنهان است.

یکی از این قابلیت‌های پنهان مرورگر، دریافت فرمان‌های خاص با استفاده از نوار آدرس است. به عبارت دقیق‌تر مرورگر کروم قادر است مجموعه فرمان‌های مختلفی را با استفاده از نوار آدرس و تایپ عبارت chrome:// در اختیار شما قرار دهد که یکی از این فرمان‌ها نیز برای ریاستارت کردن سریع مرورگر کاربرد دارد. این فرمان به شرح زیر است:

chrome://restart

اکنون که با این فرمان آشنا شدید می‌توانید به صورت یک ترفند برای ریاستارت کردن سریع مرورگر از آن کمک بگیرید، ولی برای ساده‌تر شدن کار نیز یک ترفند دیگر را با این ترفند ترکیب می‌کنیم تا این فرمان را به فهرست سایت‌های دلخواه در مرورگر اضافه کنیم و بدون نیاز به تایپ فرمان، با یک کلیک روی آن، دستور ذکر شده را

فراخوانی کنید. برای استفاده از این ترفند به این روش عمل کنید:

پیش از هر چیز مطمئن شوید نوار بوکمارکها در مرورگر فعال است. برای اطمینان می‌توانید کلیدهای Ctrl+Shift+B را فشار دهید.

حالا به یک سایت دلخواه مراجعه کرده و آیکون آن را از سمت چپ نوار آدرس با روش کشیدن و رها کردن به داخل نوار بوکمارک انتقال دهید.

روی گزینه اضافه شده به نوار بوکمارک کلیک راست ماوس را فشار داده و گزینه Edit را انتخاب کنید.

در بخش Name عنوانی دلخواه همچون «ریاستارت کروم» را وارد کنید.

در بخش URL نیز عبارت زیر را وارد کنید:

`chrome://restart`

با کلیک روی Save تغییرات را ذخیره کنید.

از حالا به بعد برای ریاستارت سریع مرورگر کافی است روی گزینه ایجاد شده در نوار بوکمارک یکبار کلیک کنید.