

معرفی نمونه اولیه کوچکترین حافظه ۱ ترابایتی دنیا



به گزارش ایسنا و به نقل از انگجت، شرکت "سندیسک" نمونه اولیه کوچکترین حافظه دنیا با ظرفیت یک ترابایت را در نمایشگاه CES 2018 رونمایی کرد.



این حافظه جدیدترین محصول معرفی شده شرکت "سندیسک" در نمایشگاه CES 2018 است که سنت این شرکت مبنی بر کوچکسازی حافظه را ادامه داده و یک دانگل یک ترابایتی با قابلیت سازگاری با پورت USB-C برای لپتاپها یا تبلتها و موبایلهای اندرویدی آینده معرفی کرده است.

ویژگی بارز این دانگل سازگاری با پورت USB-C است که انتقال اطلاعات را سرعت میبخشد.

هنوز مشخص نیست که این نمونه اولیه چه زمانی به تولید انبوه میرسد، چه وقت به بازار میآید و یا اینکه چه قیمتی خواهد داشت.

ده مسنجر معتبر و امن دنیا !!!



نسل جدید کیبورد های مجازی



http://niakanco.ir/wp-content/uploads/doc_2017-12-14_12-05-00.mp4

اگر تایپ کردن با صفحه موبایل سخت هست، نسل جدید کیبوردهای مجازی این کار را برای شما آسان کرده اند.

ایران پرچم دار انقلاب صنعتی چهارم

1	ایران	2017	100
2	ایران	2017	100
3	ایران	2017	100
4	ایران	2017	100
5	ایران	2017	100
6	ایران	2017	100
7	ایران	2017	100
8	ایران	2017	100
9	ایران	2017	100
10	ایران	2017	100
11	ایران	2017	100
12	ایران	2017	100
13	ایران	2017	100
14	ایران	2017	100
15	ایران	2017	100
16	ایران	2017	100
17	ایران	2017	100
18	ایران	2017	100
19	ایران	2017	100
20	ایران	2017	100
21	ایران	2017	100
22	ایران	2017	100
23	ایران	2017	100
24	ایران	2017	100
25	ایران	2017	100
26	ایران	2017	100
27	ایران	2017	100
28	ایران	2017	100
29	ایران	2017	100
30	ایران	2017	100
31	ایران	2017	100
32	ایران	2017	100
33	ایران	2017	100
34	ایران	2017	100
35	ایران	2017	100
36	ایران	2017	100
37	ایران	2017	100
38	ایران	2017	100
39	ایران	2017	100
40	ایران	2017	100
41	ایران	2017	100
42	ایران	2017	100
43	ایران	2017	100
44	ایران	2017	100
45	ایران	2017	100
46	ایران	2017	100
47	ایران	2017	100
48	ایران	2017	100
49	ایران	2017	100
50	ایران	2017	100

وزیر ارتباطات با انتشار آمار کسبوکارهای اینترنتی به تفکیک استانی در اینستاگرامش نوشت:
با رفع موانع، ایران پرچم دار

۱ انقلاب صنعتی چهارم در منطقه
خواهد بود.



رتبه در بهمن ۹۵	رتبه در مرداد ۹۶	نام شهر	تعداد در مرداد ۹۶	تعداد در بهمن ۹۵
۱	۱	تهران	۱۳۴۹۲	۱۰۶۵۷
۲	۲	خراسان رضوی	۲۲۷۲	۱۸۰۹
۳	۳	اصفهان	۲۲۲۴	۱۷۸۰
۴	۴	فارس	۱۵۲۹	۱۱۸۱
۵	۵	آذربایجان شرقی	۱۰۶۰	۸۳۹
۶	۶	البرز	۹۳۹	۷۵۰
۷	۷	مازندران	۷۴۵	۵۷۹
۸	۸	گیلان	۶۶۷	۵۴۹
۹	۹	خوزستان	۶۱۵	۴۸۷
۱۰	۱۰	قم	۵۷۵	۴۷۹
۱۱	۱۱	آذربایجان غربی	۴۹۵	۴۱۰
۱۲	۱۲	یزد	۴۸۶	۳۸۴
۱۳	۱۳	هرمزگان	۴۱۹	۳۲۳
۱۴	۱۴	کرمان	۳۷۹	۳۰۰
۱۶	۱۵	گلستان	۳۰۱	۲۳۲
۱۵	۱۶	قزوین	۲۹۰	۲۴۲
۱۸	۱۷	مرکزی	۲۷۵	۲۱۵
۱۷	۱۸	بوشهر	۲۵۵	۲۱۷
۱۹	۱۹	اردبیل	۲۳۷	۱۹۹
۲۱	۲۰	کرمانشاه	۲۳۷	۱۸۶
۲۰	۲۱	کردستان	۲۳۲	۱۸۹
۲۲	۲۲	همدان	۲۲۵	۱۷۴
۲۴	۲۳	زنجان	۲۱۵	۱۵۸
۲۳	۲۴	سمنان	۲۱۱	۱۶۸
۲۵	۲۵	خراسان جنوبی	۱۷۸	۱۴۲
۲۶	۲۶	لرستان	۱۳۲	۹۹
۲۷	۲۷	چهارمحال و بختیاری	۱۱۶	۸۷
۲۸	۲۸	خراسان شمالی	۱۱۳	۸۳
۲۹	۲۹	سیستان و بلوچستان	۱۰۲	۷۸
۳۰	۳۰	کهگیلویه و بویراحمد	۵۳	۴۴
۳۱	۳۱	ایلام	۵۱	۴۴

مقایسه رتبه تعداد کسب و کارهای استان
ها نسبت به رتبه آنها در بهمن ۹۵

رتبه برابر رتبه بالاتر رتبه پایین تر

پرینت گرفتن دو صفحه در یک صفحه در Word

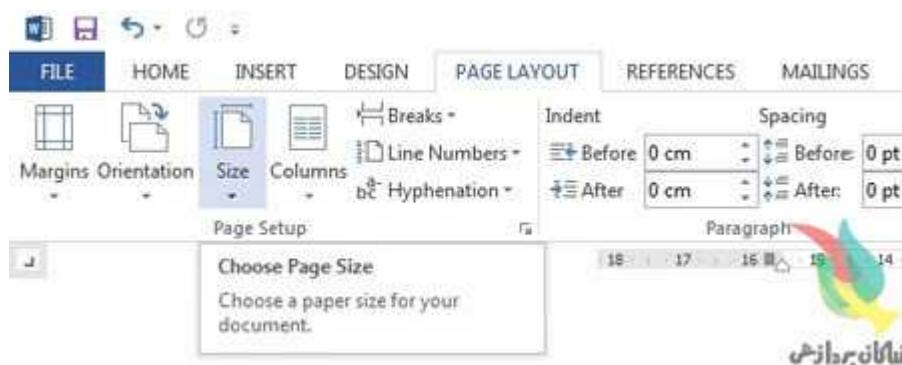


در زمان پرینت گرفتن برخی اسناد در ورد گاهی احتیاج پیدا می کنیم به علت کمبود کاغذ ، دو صفحه را در یک صفحه پرینت کنیم. یا زمان هایی پیش می آید که می خواهیم یک جزوه را در ابعاد کوچکتر چاپ کنیم. به عبارت دیگر در این مقاله خواهید آموخت که چگونه دو صفحه A5 را در یک صفحه A4 پرینت بگیرید.

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

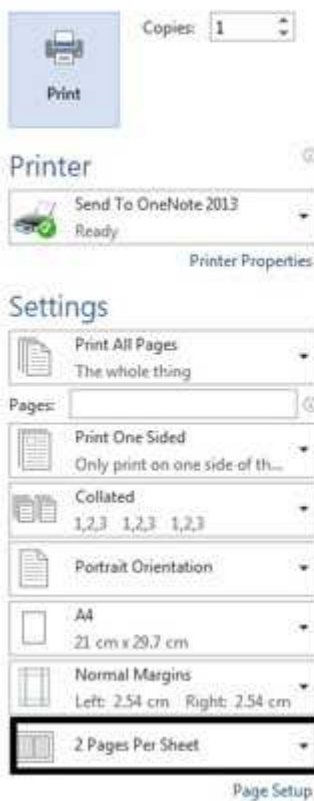
روش تنظیم کردن کاغذ و ابعاد پرینت

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



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.

دسترسی به عکسهای پاک شده در تلفن همراه



برخلاف تصور شما عکسهای پاک شده در تلفن همراهتان به راحتی قابل دسترسی اند!

دسترسی دوباره به عکسهایی که از تلفن هوشمندتان پاک می‌کنید، بسیار آسان بوده و همین موضوع می‌تواند گاهی اوقات بسیار مشکل‌ساز باشد.

برای مثال حالتی را در نظر بگیرید که می‌خواهید گوشی خود را که صدها عکس شخصی در آن ذخیره کرده‌اید، بفروشید. در این وضعیت خیلی راحت وارد گالری می‌شوید و با انتخاب گزینه Delete All همه عکسها را پاک می‌کنید و یا کل گوشی را ریست فکتوری می‌کنید.

در این حالت با این فکر که عکسهایتان برای همیشه پاک شده، گوشی را تحویل شخص خریدار می‌دهید. اما چیزی که خبر ندارید این است که شخص خریدار به راحتی می‌تواند با این روش، به تمامی عکسهای ذخیره شده شما در حافظه داخلی، دسترسی پیدا کند.

اما برای جلوگیری از این موضوع چه کاری باید انجام داد؟

در واقع شما باید با انجام عملیاتی، عکسها را به صورتی پاک کنید که در آینده با هیچ روشی قابل بازگردانی نباشند.

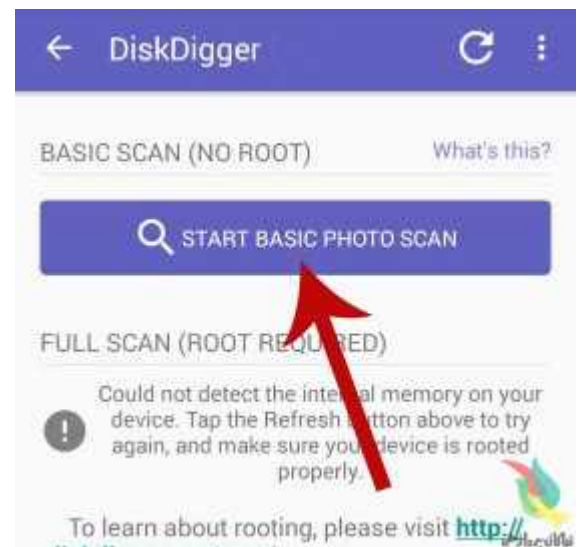
برای انجام این کار در گوشی‌های اندرویدی مراحل زیر را به ترتیب طی کنید:

عکسهایتان را به همان روش معمولی با انتخاب گزینه Delete در گالری، حذف نمایید.

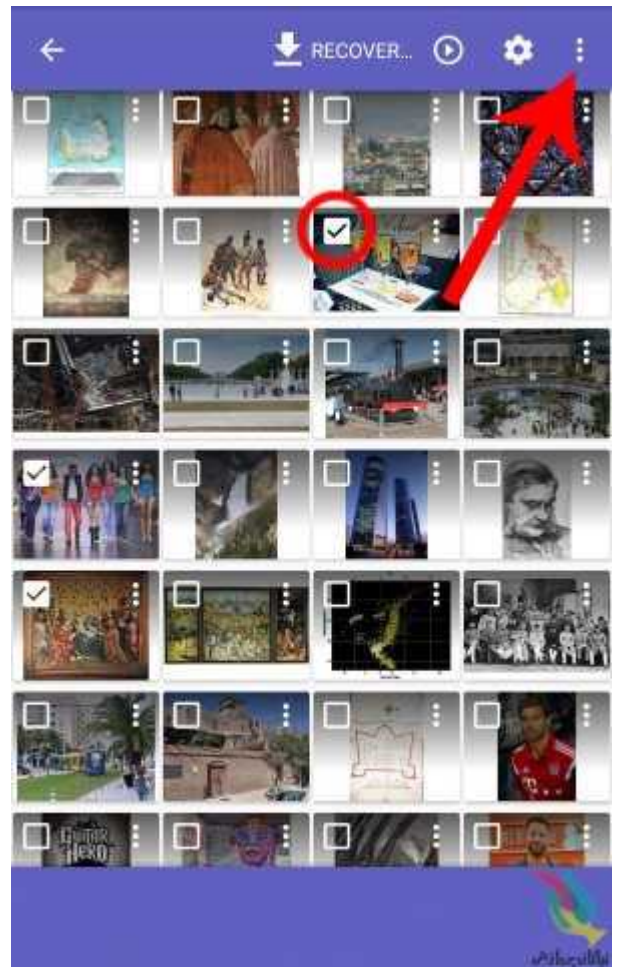
اپ DiskDigger را از اپاستور دانلود و نصب کنید. این برنامه در

دو نسخه رایگان و Pro موجود بوده که در این آموزش از نسخه رایگان آن استفاده شده است.

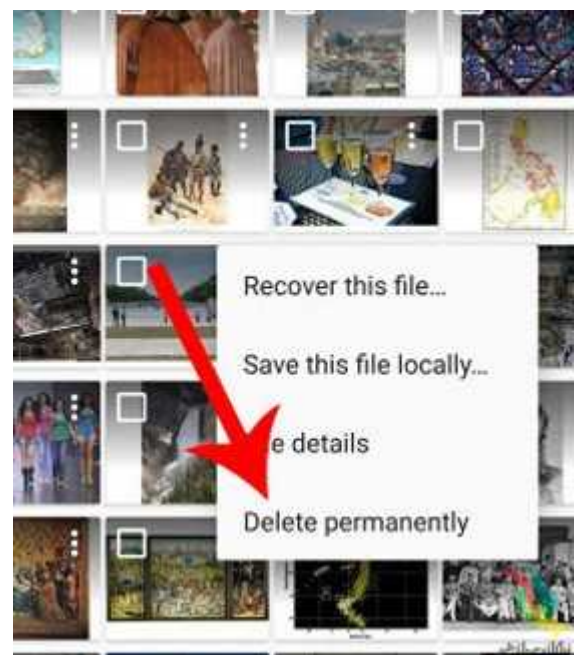
برنامه را باز کرده و روی START BASIC PHOTO SCAN کلیک کنید. با این کار تمامی تصاویر حذف شده‌ای که قابل بازگردانی هستند نمایان خواهند شد. دقت داشته باشید که اگر گوشی شما روت شده باشد، درصد خطای این برنامه در پیدا کردن تصاویر حذف شده، به حداقل خواهد رسید.



پس از مدتی انتظار، می‌توانید عکسهای حذف شده را مشاهده کنید. در این مرحله عکسهای را که می‌خواهید به‌طور کامل از دستگاه شما پاک شوند، انتخاب کنید.



بر روی آیکن سه نقطه کلیک کرده و گزینه Delete Permanently را برگزینید.



در این حالت تصاویری که انتخاب کرده‌اید، به‌طور دائمی و بدون شانس بازگشت، پاک خواهند شد.

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 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 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 مارکتهای 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 بيفتید، 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!

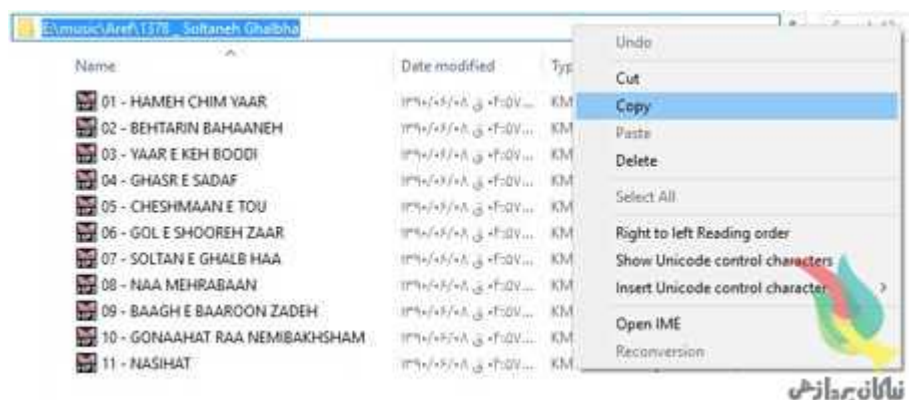
نکته سوم ارتباطی به خود بدافزارها پیدا نمی‌کند، اما در هر صورت لازم است همیشه از داده‌های روی تلفن همراه‌تان بک‌آپ بگیرید و تا حد امکان از نگهداری داده‌های حساس روی آن خودداری کنید تا اگر اتفاقی چه نرم‌افزاری و چه سخت‌افزاری افتاد، فهرست نگرانی‌هایتان شامل از بین رفتن یا دزدی اطلاعات خصوصی نباشد!

تغییر دسته‌جمعی نام فایل‌ها در محیط ویندوز به کمک اکسل

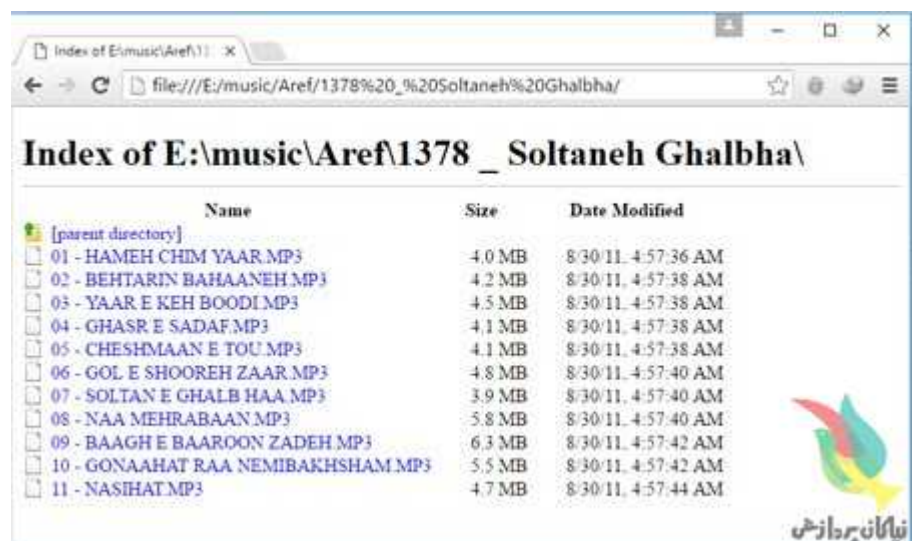
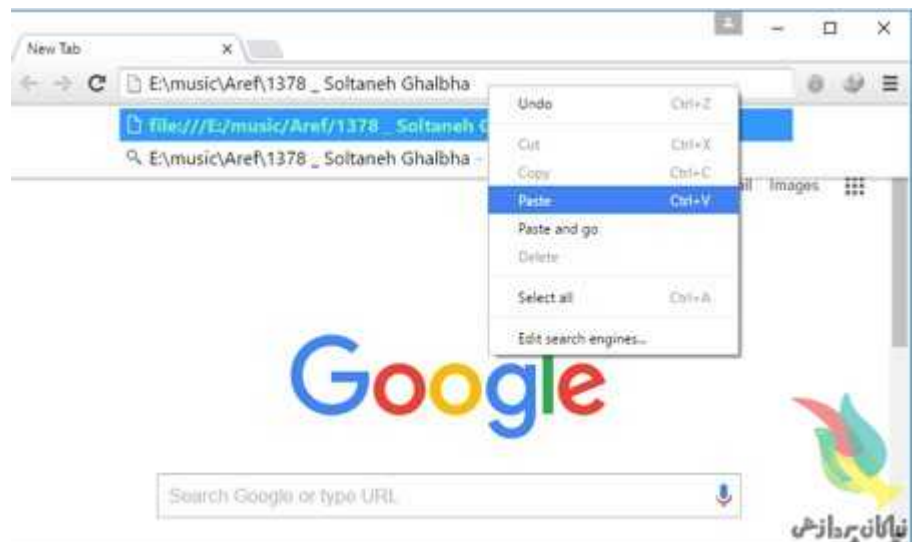


در این ترفند به نحوه‌ی تغییر دسته‌جمعی و یکجای نام فایل‌ها در محیط ویندوز به کمک نرم‌افزار مایکروسافت اکسل و Command Prompt خواهیم پرداخت. این روش از نام‌های فارسی نیز پشتیبانی می‌کند.

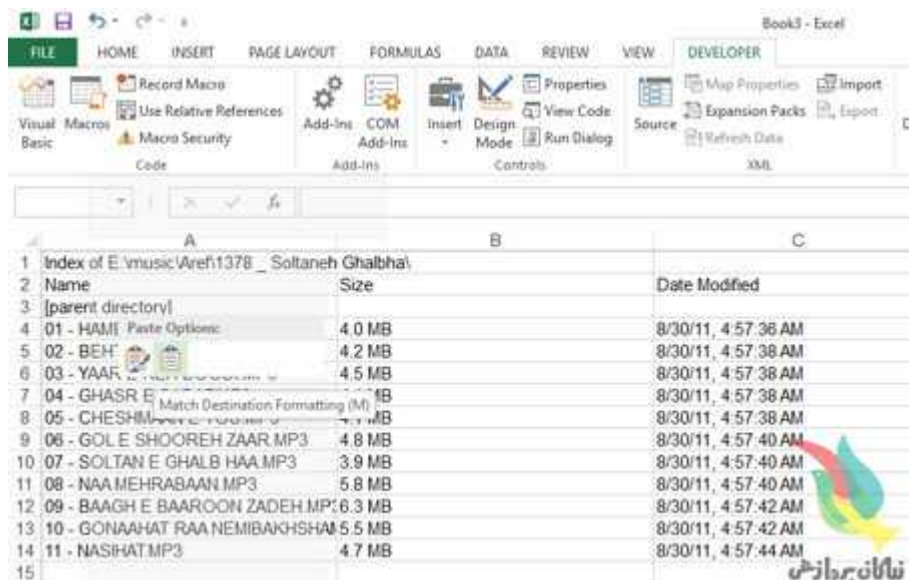
ابتدا وارد پوشه‌ای که فایل‌ها در آن قرار دارد شوید. سپس مسیر پوشه را Copy کنید.



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

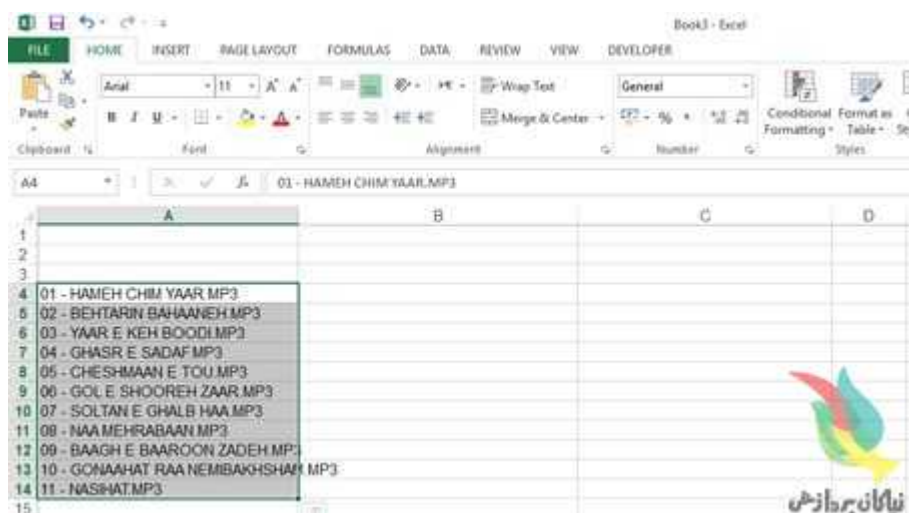


اکنون توسط کلیدهای ترکیبی Ctrl+A کل متون صفحه را انتخاب کرده و آنها را Copy کنید. سپس داخل محیط اکسل در یک صفحه جدید، این محتوا را Paste نمایید.



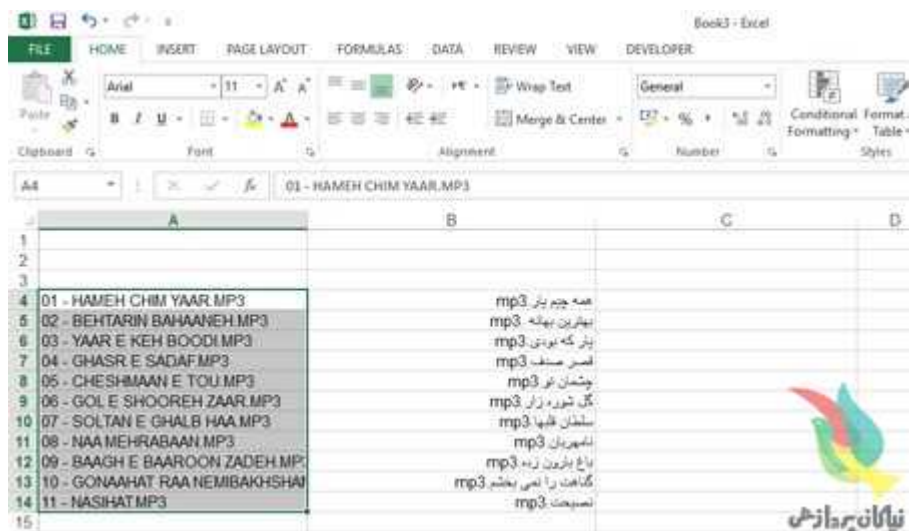
	A	B	C
1	Index of E:\music\Aref1378 _ Soltane Ghalibhai		
2	Name	Size	Date Modified
3	[parent directory]		
4	01 - HAMEH CHIM YAAR.MP3	4.0 MB	8/30/11, 4:57:38 AM
5	02 - BEHTARIN BAHANEH.MP3	4.2 MB	8/30/11, 4:57:38 AM
6	03 - YAAR E KEH BOODI.MP3	4.5 MB	8/30/11, 4:57:38 AM
7	04 - GHASR E SADAF.MP3	4.1 MB	8/30/11, 4:57:38 AM
8	05 - CHESHMAAN E TOU.MP3	4.1 MB	8/30/11, 4:57:38 AM
9	06 - GOL E SHOOREH ZAAR.MP3	4.8 MB	8/30/11, 4:57:40 AM
10	07 - SOLTAN E GHALB HAA.MP3	3.9 MB	8/30/11, 4:57:40 AM
11	08 - NAA MEHRABAAN.MP3	5.8 MB	8/30/11, 4:57:40 AM
12	09 - BAAGH E BAAROOON ZADEH.MP3	6.3 MB	8/30/11, 4:57:42 AM
13	10 - GONAAHAT RAA NEMIBAKHSHAM.MP3	5.5 MB	8/30/11, 4:57:42 AM
14	11 - NASHAT.MP3	4.7 MB	8/30/11, 4:57:44 AM
15			

سلول‌های اضافی را پاک نمایید.

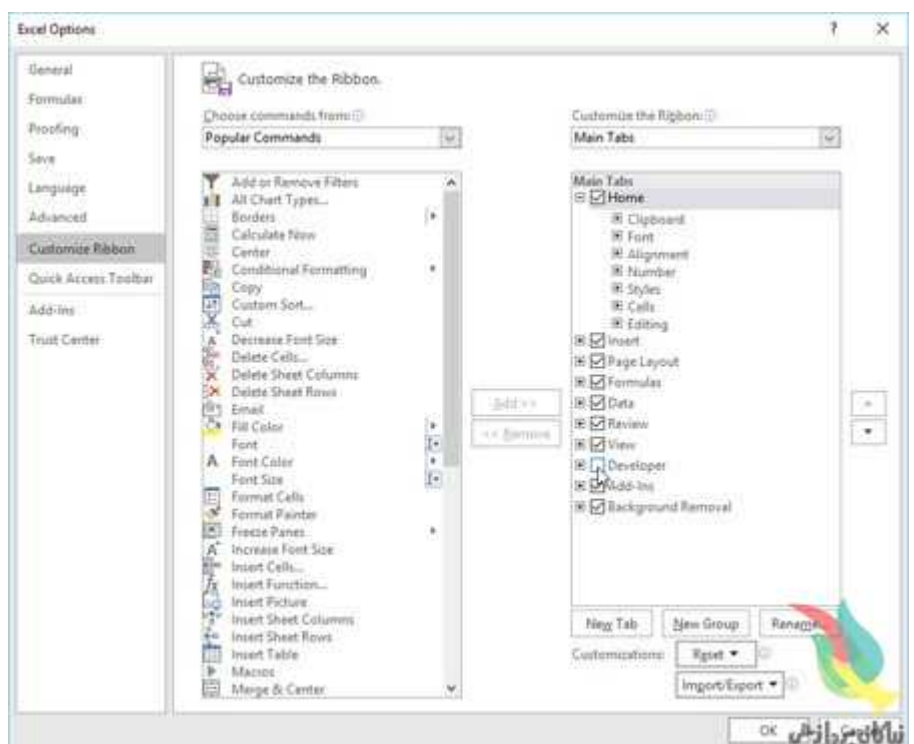


	A	B	C	D
1				
2				
3				
4	01 - HAMEH CHIM YAAR.MP3			
5	02 - BEHTARIN BAHANEH.MP3			
6	03 - YAAR E KEH BOODI.MP3			
7	04 - GHASR E SADAF.MP3			
8	05 - CHESHMAAN E TOU.MP3			
9	06 - GOL E SHOOREH ZAAR.MP3			
10	07 - SOLTAN E GHALB HAA.MP3			
11	08 - NAA MEHRABAAN.MP3			
12	09 - BAAGH E BAAROOON ZADEH.MP3			
13	10 - GONAAHAT RAA NEMIBAKHSHAM.MP3			
14	11 - NASHAT.MP3			
15				

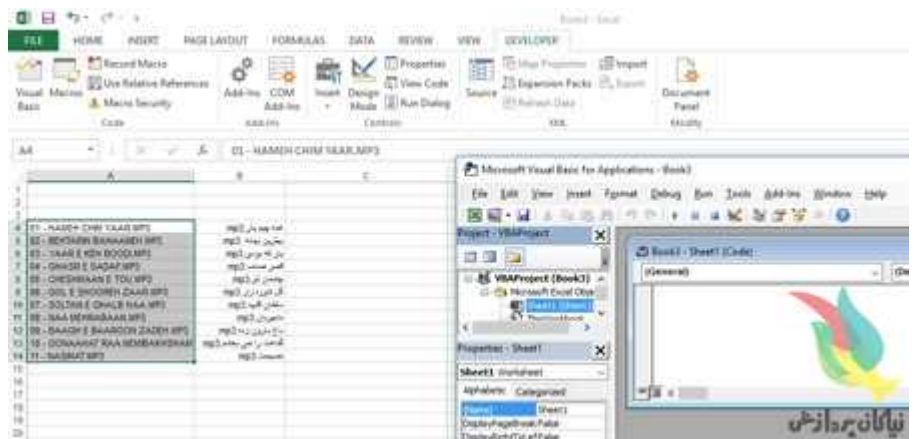
نام جدید با فرمت‌شان را در ستون مقابل بنویسید. سپس ستون نام قدیمی فایل‌ها را انتخاب کنید.



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 دوبار کلیک کنید تا پنجره‌ی سفید رنگ برنامه نویسی باز شود.



کد زیر را در کادر سفیدرنگ Paste نمایید:

()Sub Macro1

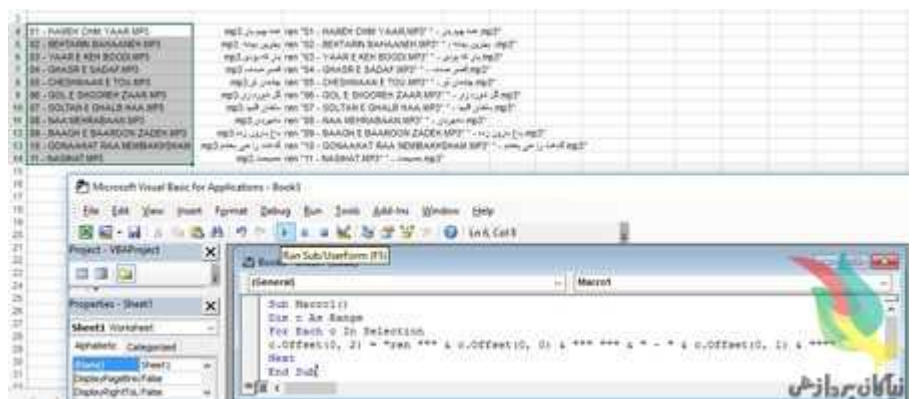
Dim c As Range

For Each c In Selection

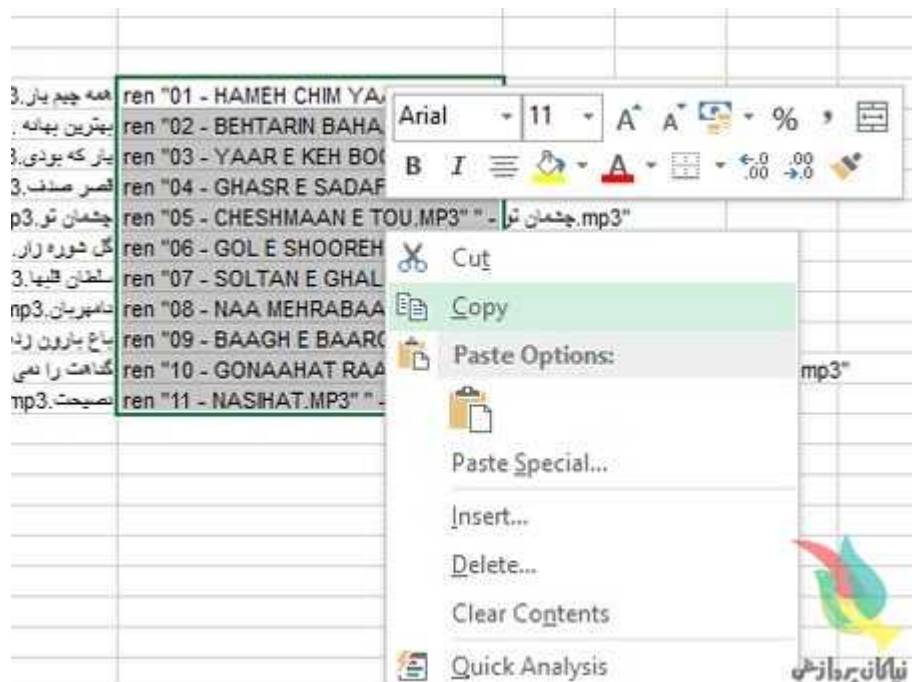
c.Offset(0, 2) = "ren " & c.Offset(0, 0) & " " & " - " & " " & (c.Offset(0, 1

Next

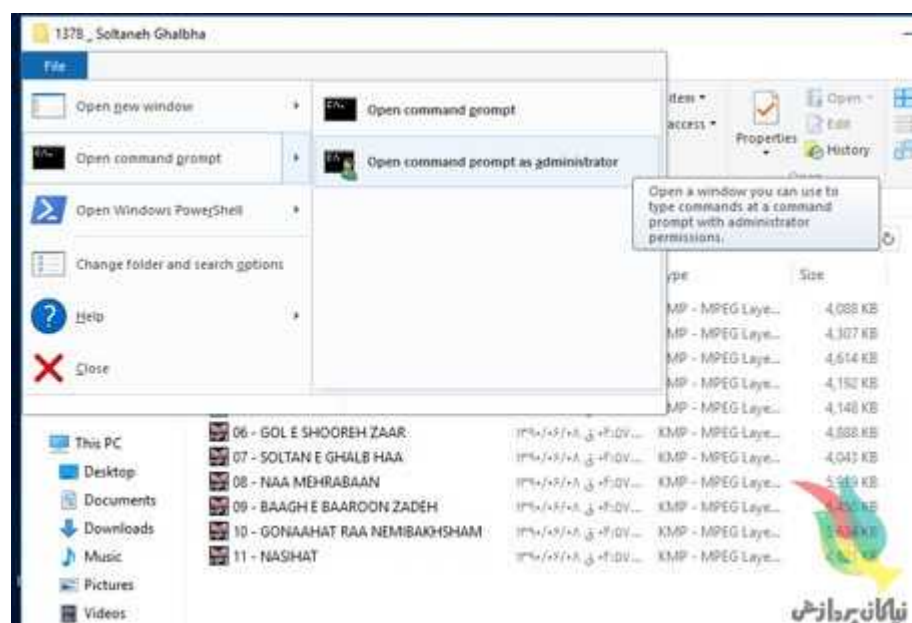
End Sub



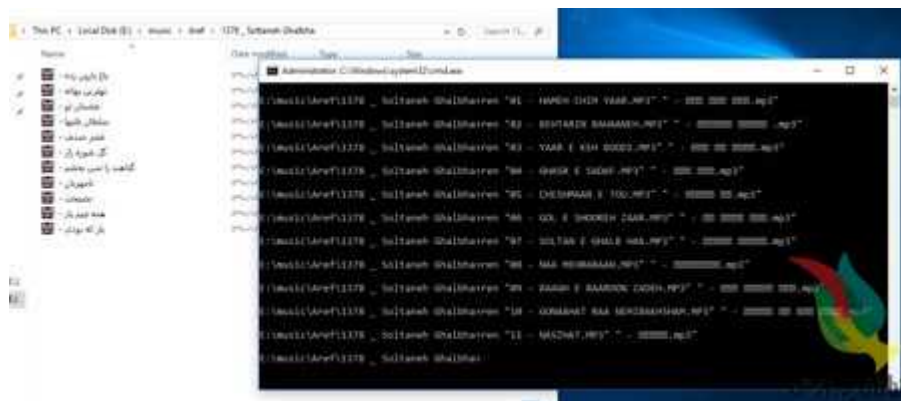
ستون ایجاد شده را Copy نمایید.



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 سوء 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.



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



۱۱۳ گوشی هوشمند در آمریکا در هر دقیقه گم می‌شود.



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



۳۵۰,۰۰۰ ویروس اندرویدی توسط Sophos Labs دیده شده است.

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 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.