

ترفند ویندوز |

فایل‌های مخفی شده با ویروس را نمایان کنید



این روزها ویروس‌های رایانه‌ای علاقه زیادی به مخفی کردن فایل‌های شخصی کاربر دارند! بسیاری از ویروس‌ها، فایل‌های روی فلش و هاردهای اکسترنال را مخفی می‌کنند؛ اما مشکل اصلی آن جاست که با راست کلیک کردن بر روی فایل‌های مخفی شده و رفتن به Properties آن‌ها، متوجه می‌شوید که قادر به برداشتن تیک گزینه Hidden نیستید! این اتفاق به خاطر این می‌افتد که ویروس، فایل‌ها را سیستمی می‌کند و به همین علت قادر به برداشتن تیک Hidden در حالت عادی نیستید. در این هفته برای شما روشی را به شما بازگو می‌کنیم که با یک کلیک بتوانید این فایل‌های سمج را از حالت مخفی خارج کنید. لازم به ذکر است که برای این کار راه‌حل‌های متفاوتی وجود دارد اما به شما راه‌حلی را خواهیم گفت که سریع‌تر و کوتاه‌تر از دیگر راه‌حل‌ها می‌باشد.

برای این کار با فشردن کلیدهای ترکیبی Win+R وارد Run شده و در فیلد مربوطه عبارت notepad را وارد کرده و Enter بزنید. در محیط Notepad متن زیر را عیناً تایپ کنید:

```
echo off@
echo
echo Created by www.TARFANDESTAN.com
echo
echo
echo
echo Warning: DO NOT run this file in Windows drive
pause
echo
echo attrib -s -h *.* /s /D
echo Success
echo
echo
echo
echo
echo
echo Save as منوی File گزینه Save As را انتخاب کنید. در پنجره باز شده از قسمت type گزینه All Files را انتخاب کنید و در فیلد File name نام فایل را با پسوند BAT ذخیره کنید. حال فایل BAT را به فلش دیسک یا هر پوشه دیگری در رایانه که محتوی فایل‌های مخفی شده است منتقل کنید. با اجرای فایل BAT صفحه Command Prompt باز می‌شود. با فشردن هر کلیدی، عملیات شروع شده و در چند ثانیه تمام فایل‌های مخفی شده نمایان می‌شوند.
```

احتمال هک شدنتان را کمتر کنید

نکاتی برای کاهش هک شدن وای‌فای شما

۵- از یک نرم‌افزار Firewall قدرتمند استفاده کنید. فایروال‌ها با بستن پورت‌های اضافی بر روی ویندوز، راه‌ها را برای هکرها مسدود و تنگ می‌کنند. معمولاً بسیاری از افراد ترجیح می‌دهند که از فایروال ویندوز استفاده کنند اما بد نیست که گزینه‌های دیگری مانند Zone Alarm را نیز تست کنید. این نرم‌افزار به شما اطلاعات مفیدی ارائه می‌کند. مثلاً لیست تمامی برنامه‌هایی که از اینترنت استفاده می‌کنند را در اختیار شما قرار می‌دهد.

۶- هرگز رمز عبور خود را تا جای ممکن به دوستان و آشنایان جهت استفاده از مودم ندهید. سعی کنید در صورت تمایل، خودتان رمز عبور را وارد دستگاه آن‌ها کنید.

۷- برخی شرکت‌های سرویس‌دهنده اینترنت، سرویسی را فراهم می‌کنند تا هر کاربر تنها با یک MAC Address بتواند به اینترنت متصل شود. در صورتی که تنها از یک رایانه برای اتصال به اینترنت استفاده می‌کنید با استفاده از این سرویس می‌توانید اطمینان پیدا کنید فقط خودتان هستید که می‌توانید به مودم متصل شوید و از اینترنت استفاده کنید.

۸- همان‌طور که در ابتدای مطلب هم گفتیم یکی از بهترین کارها این است که در زمان‌هایی که از خانه یا محل کار به مدت طولانی خارج می‌شوید می‌توانید به راحتی مودم خود را خاموش کنید.

۹- شما می‌توانید با مراجعه به سایت سازنده مودم، آخرین نسخه Firmware مودم را نصب کنید تا تنظیمات نرم‌افزاری مودم شما نیز همواره به‌روز باشد.

۱۰- اگر رایانه شما نزدیک به مودم است و می‌توانید از سیم برای اتصال به آن استفاده کنید، با اتصال سیم به مودم می‌توانید تنظیمات مربوط به اتصال بی‌سیم را در مودم غیرفعال کنید.

راه‌حل مطمئن‌ترین روشی است که می‌توانید جلوی دسترسی دیگران به اینترنت خود را بگیرید اما اگر دوست ندارید دائماً درگیر روشن یا خاموش کردن مودم خود باشید این هفته به شما نکاتی را آموزش خواهیم داد که با رعایت آن‌ها می‌توانید تا حد بسیار زیادی جلوی دسترسی هکرها و همچنین افراد عادی را به مودم وای‌فای خود بگیرید. در ادامه به معرفی ۱۰ نکته برای پیش‌گیری از هک شدن اتصالات بی‌سیم خواهیم پرداخت.

۱- یکی از شرکت‌هایی که همیشه برای حل این مشکل راه‌حل‌هایی را پیشنهاد می‌کند، مایکروسافت است. به پیشنهاد شرکت مایکروسافت توجه کنید؛ مایکروسافت می‌گوید بهترین نوع رمزگذاری روی مودم شبکه بی‌سیم، پروتکل‌های امنیتی WPA-PSK و PSK-WPA2 هستند. این نوع پروتکل‌ها، رمز عبور شما را هر میلی‌ثانیه رمزگذاری می‌کنند و درصد هک آن را به ۶۴ سال آینده موقوف می‌کنند! تعجب نکنید، این واقعیت این نوع رمزگذاری است. با استفاده از این روش می‌توانید تا مدت‌زمانی اطمینان داشته باشید که حداقل افراد عادی نمی‌توانند امنیت شما را به خطر اندازند.

۲- اگر شما از بیش از یک رایانه برای اتصال به اینترنت استفاده نمی‌کنید مودم خود را بر روی حالت Bridge تنظیم کنید.

۳- در صورت استفاده از حالت PPPoE بر روی مودم، قابلیت MAC Filter را بر روی مودم فعال کنید.

۴- برخی برنامه‌ها نظیر Wireless Network Watcher می‌توانند به شما جهت مشاهده اتصالات دستگاه‌های بی‌سیم به مودم شما پیغام هشدار دهند. در صورت مشاهده اتصالات ناشناخته آن‌ها را قطع کرده و یا هرچه سریع‌تر رمز عبور مودم خود را تغییر دهید.

خطر هک شدن، یکی از بزرگ‌ترین خطراتی است که کاربرانی که از مودم بی‌سیم برای اتصال به اینترنت استفاده می‌کنند را تهدید می‌کند. شما نیز اگر از مودم بی‌سیم برای اتصال به اینترنت استفاده می‌کنید و متوجه کم شدن غیرمعمول حجم اینترنت خود شده‌اید این امکان وجود دارد که رمز عبور مودم شما توسط هک‌هایی که در نزدیکی شما زندگی می‌کنند، هک شده باشد. بارها در بخش‌های مختلف بایت و به خصوص کانال تلگرام بایت به آموزش نکاتی در رابطه با بالا بردن امنیت مودم‌های وای‌فای پرداخته‌ایم اما باز هم مشکلات بسیار زیادی در این رابطه وجود دارد. متأسفانه هر روز نرم‌افزارهای جدیدی به بازار وارد می‌شوند که کارشان پیدا کردن مودم‌های مختلف و هک کردن آن‌هاست. این نرم‌افزارها به سادگی در اختیار افراد عادی هم قرار می‌گیرند و با این اوصاف کسی که از اینترنت شما و از مودم شما استفاده می‌کند، لزوماً یک هکر حرفه‌ای نیست. خیلی از افراد این روزها با داشتن نرم‌افزارهایی نظیر Andro Dumper می‌توانند به سادگی بدون این که پسورد مودم شما را داشته باشند، از مودم و همچنین اینترنت شما استفاده کنند. اگر شما هم جزو آن دسته از افرادی هستید که از شما در این زمینه سوء استفاده شده است احتمالاً تا به خودتان می‌آید، می‌بینید که حجم اینترنت مصرفی شما به پایان رسیده است و مجبور هستید که دوباره اینترنت خود را شارژ کنید. باید بدانید که اگر این مشکلات گریبانگیرتان شده است، راه‌حلی وجود دارد که تا حد امکان مودمتان را از دسترس افراد سودجو دور نگه دارید. شاید بد نباشد که قبل از هر چیز بگوییم بهتر است در زمان‌هایی که خانه نیستید یا از اینترنت خود استفاده نمی‌کنید، مودمتان را خاموش کنید. بدون شک این

سفارش اینترنتی آگهی

صرفاً جویند در وقت و هزینه

www.37010.ir

۵٪ تخفیف مازاد در نیازمندها
سفارش ۲۴ ساعته / پرداخت آنلاین

