

بسمه تعالی

امنیت در USB Flash Drive

فهرست مطالب

۱. مقدمه ۲
۲. دسترسی به Flash Drive ۲
۳. فقط خواندنی کردن حافظه ۳
۴. رمزنگاری داده ها ۴

مقدمه

یکی از مباحث مهم در امنیت اطلاعات شخصی، محافظت از داده‌ها بر روی حافظه‌های کوچک همراه یا همان Flash Drive ها می باشد که غالباً همراه سیستم اتصالاتی USB می باشند. این گونه حافظه‌های همراه از چند نظر مورد آسیب پذیری قرار می گیرند. از بین رفتن داده‌ها و یا ویروسی شدن آنها از شایعترین موارد آسیب پذیری داده‌های این گونه حافظه‌ها می باشد. در ادامه به بررسی سه موضوع اصلی و مهم در مورد امنیت در این گونه حافظه‌های همراه می پردازیم.

دسترسی به Flash Drive

اولین مبحث مهم در این موضوع، بررسی ساختاری است که دسترسی به این گونه حافظه‌ها را محدود به افرادی بکند که اجازه دسترسی به داده‌های آن را دارند. یکی از بهترین راه‌کارها برای این موضوع، قرار دادن یک گذرواژه امنیتی برای دسترسی به Flash Drive می باشد. این کار بدین صورت می باشد که توسط یک نرم افزار مخصوص، می توانید یک Password بر روی Flash Memory خود قرار دهید تا هنگامی که حافظه را به هر سیستمی متصل می کنید، برای دیدن داده‌های محتوای حافظه، یک گذرواژه را از کاربر درخواست می کند و فقط در حالتی می توان به Flash Memory دسترسی داشت که گذرواژه صحیح را وارد نمود. یکی از نرم افزارهای معروف در این زمینه، نرم افزار Gilisoft USB Stick Encryption می باشد که تصویری از این نرم افزار را در زیر مشاهده می فرمایید.

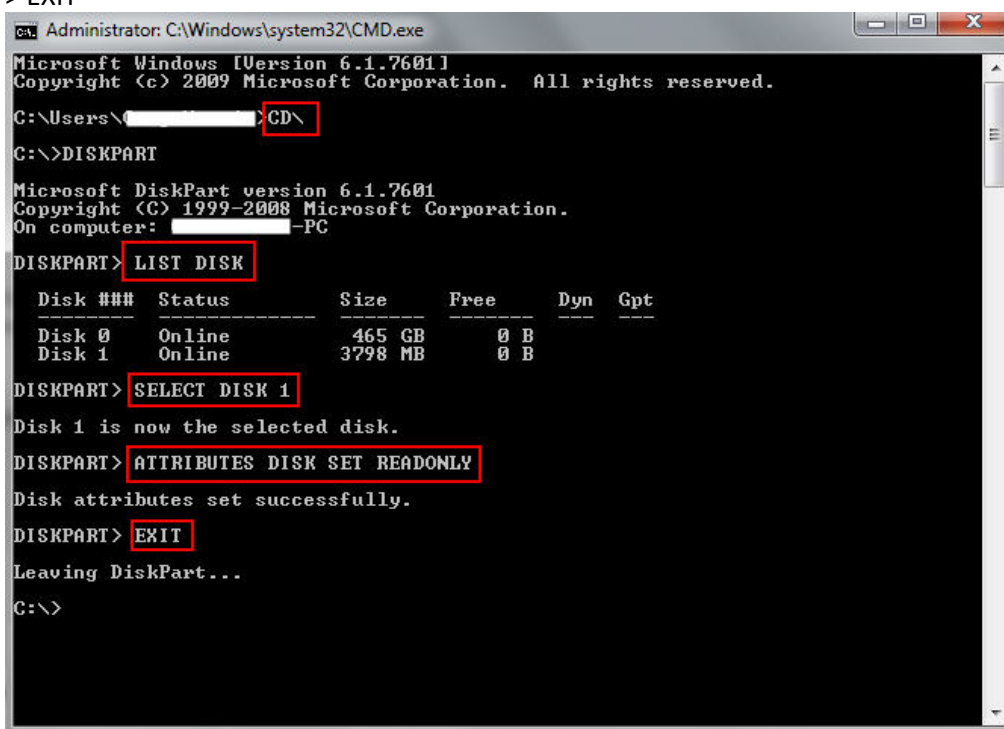


فقط خواندنی کردن حافظه

یکی از مسائل مهم در نگهداری فایل ها و داده های مهم بر روی حافظه در مقابل ویروسی شدن آنها، این است که پس از قرار دادن داده های مهم خود بر روی حافظه، حافظه را فقط خواندنی یا همان Read Only کنیم. برای این کار هم می توان از دستورات سیستمی استفاده کرد و هم می توان از ابزارهایی که برای این کار طراحی شده اند استفاده کرد.

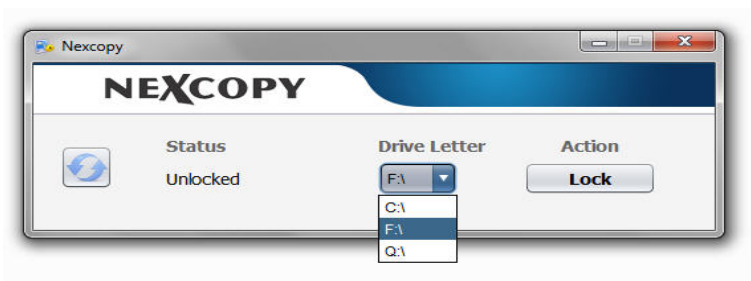
در ابتدا می خواهیم دستورات سیستمی DISKPART را توضیح دهیم. ابتدا توسط دستور List Disk نام و شماره دیسک مورد نظر را پیدا می کنیم و بعد از انتخاب کردن آن، با استفاده از دستور Attributes دیسک مورد نظر را فقط خواندنی می کنیم.

```
C:\> cd\  
C:\> DISKPART  
DISKPART> LIST DISK  
DISKPART> SELECT DISK 1  
DISKPART> ATTRIBUTES DISK SET READONLY  
DISKPART> EXIT
```



```
Administrator: C:\Windows\system32\CMD.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\> CD\  
C:\> DISKPART  
Microsoft DiskPart version 6.1.7601  
Copyright (C) 1999-2008 Microsoft Corporation.  
On computer: -PC  
DISKPART> LIST DISK  
Disk ### Status Size Free Dyn Gpt  
Disk 0 Online 465 GB 0 B  
Disk 1 Online 3798 MB 0 B  
DISKPART> SELECT DISK 1  
Disk 1 is now the selected disk.  
DISKPART> ATTRIBUTES DISK SET READONLY  
Disk attributes set successfully.  
DISKPART> EXIT  
Leaving DiskPart...  
C:\>
```

اگر نمی خواهید از دستورات سیستمی استفاده کنید، می توانید از نرم افزار Nexcopy USB WriteProtect استفاده کنید. این نرم افزار همان کاری را می کند که دستورات بالا انجام می دهد. به عبارت دیگر کل حافظه Flash Drive را Read Only می کند. تصویر این نرم افزار را در زیر مشاهده می فرمایید.



رمزنگاری داده ها

از دیگر راه های مراقبت از فایلها و داده های مهم بر روی حافظه های همراه در مقابل دسترسی غیرمجاز و یا دستکاری و ویروسی شدن داده ها، رمزنگاری داده ها می باشد. برای انجام رمزنگاری داده ، بهترین راه استفاده از نرم افزارهای مطمئنی است که هم دارای الگوریتم های قوی باشد و هم اینکه این نرم افزار در بین کاربران بسیاری در دنیا شناخته شده باشد. یکی از این گونه نرم افزارها، نرم افزار idoo File Encryption می باشد که از الگوریتم AES-256 جهت رمزنگاری فایلها و داده ها استفاده می کند. این نرم افزار علاوه بر قابلیت رمزنگاری فایلها، دارای قابلیت پاک کردن فایلها به صورت غیربازگرداننده یا همان Shredder کردن فایلها را دارا می باشد. تصویری از این برنامه را در زیر مشاهده می فرمایید:

