

## \* به نام خدا \*

هک پسورد ویندوز ها (XP , 7 , 8 , 8.1 , 10 و...) به روش های مختلف

میدونم بعضیاتون گاهی اوقات براتون پیش اومد که رمزتون ویندوزتون رو فراموش کردید و نتونستید وارد سیستمتون بشید. البته بعضیا هم به قصد دیگه ای دارن!!! برخی با این اتفاق به فکر این می افتن که ویندوزشون رو عوض کنن. اوووو کی حوصله داره این همه دوباره ویندوز نصب کنه و برنامه ها رو نصب کنه و حتی بعضی فایل هایی که توو درایو ویندوزش هست پاک میشه و... داستان داره...

ولی چرا این همه دردسر؟!؟

در پست قبلی دوست عزیزم **Virus32** زحمت کشید روش هک کردن ویندوز رو آموزش داد. ولی چون ویروس جان سرش شلوغه، من براتون هک ویندوز اکس پی **XP** و ویندوز **V** به بالا رو به انواع روش ها آموزش میدم، توو ویندوز سون به بالا ما نیاز به یک سیدی ویندوز داریم ولی از اون طرف سرعت کار سریع تر و راحت تره.

شرکت مایکروسافت پس از ساخت ویندوز حفره های امنیتی رو توو ویندوز به جا گذاشت که البته هرچی نسخه های ویندوز بالا تر میره، حفره ها کمتر میشه و امنیت ویندوز بیشتر میشه. من امروز بهتون یاد میدم که چطور از این حفره ها بشه استفاده کرد و ویندوز رو هک کرد.

**ورود به ویندوز XP بدون پسورد**

این روزا ویندوز اکس پی **XP** داره از مد می افته ولی هنوز طرفدارای زیادی داره که هنوز از ویندوز اکس پی استفاده می کنن.

حالا اگه توو ویندوز **XP** پسورد گذاشتین و فراموشش کردین و یا... با این روش خیلی سریع و راحت می تونین وارد ویندوز بشین

**روش اول:** این روش در اکثر سیستم ها جواب میدهد. ما در این روش پسورد رو از بین نمی بریم و

عوض هم نمیکنیم در واقع از یوزری دیگه ی وارد سیستم میشیم که نامش **Administrator** هست و یوزر اصلی ویندوز می باشد. ولی بعضیا حرفه ای تر عمل می کنن و یوزر **Administrator** رو هم رمز میدن برای همین این روش برای اون سیستم ها جواب نمیده. خوب شروع میکنیم!

۱- اول کامپیوتر رو روشن کنید و منتظر بمونید تا ویندوز بالا بیاد و ازتون رمز بخواد.

۲- خوب حالا دکمه های **Alt** و **Shift** و **Delete** کیبورد رو با هم بفشارید.

۳- دوباره این کارو تکرار کنید یعنی دکمه های **Alt** و **Shift** و **Delete** کیبورد رو دوباره فشار دهید.

۴- خواهید دید که صفحه ای مانند صفحه پایین براتون ظاهر میشه.



که ازتون یوزرنیم و پسورد میخواد.

۵- کادر **User name:** و **Password:** رو خالی بزارید و هرچی نوشته شده است رو پاک کنید و توو کادر یوزرنیم بنویسید: **Administrator** توو کادر پسورد هیچی ننویسید! (مانند تصویر زیر)



۶- روی **OK** کلیک کنید یا اینتر رو بزنید.

۷- می بینید که صفحه **Welcome** ظاهر می شود و ویندوز در حال اجرا شدن هست. کمی صبر کنید و بعد از آن لذت ببرید.

تمام!

**روش دوم: (این روش همون روشی هست که داداش ویروس توو به پست گفته بود. من فقط**

**یادآوری کردم تا این کتاب کامل شه (با یسری ویرایش ها خیلی جزئی):**

۱- ابتدا سیستم رو روشن میکنیم و وقتی سیستم در حال استارت بود **"Starting Windows"** سیستم رو دوباره با دکمه پاور کیس خاموش میکنیم.

یا بوت رو دست کاری میکنیم . یا میتونیم باتری کیس رو در بیارم سیستم رو روشن کنیم دوباره خاموش کنیم باتری رو بزاریم سر جاش و ... خلاصه باید کاری کنیم تا ویندوز هنگ کنه

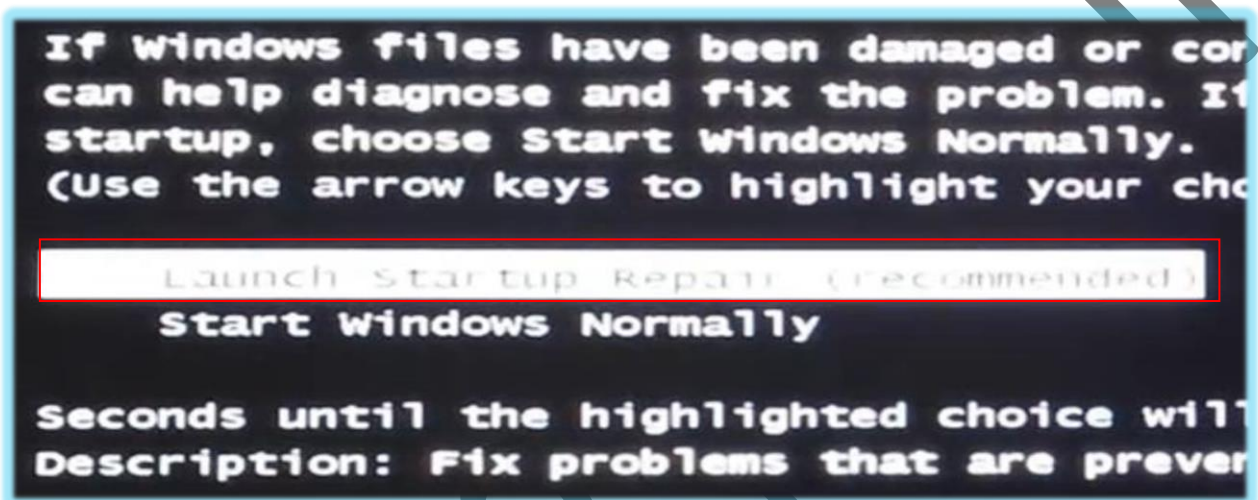
"از هر ترفند دیگه ای که به ذهنتون میرسه میتونید استفاده کنید"

Starting Windows

این عمل فقط برای ایجاد اختلال در اطلاعات ویندوز هفته چون این ویندوز یکی از آپشن هاش  
اینه که ایرادهای خودش رو پیدا کرده و برای رفع آنها تلاش میکنه و این میتونه یه نقطه ضعف هم  
باشه.

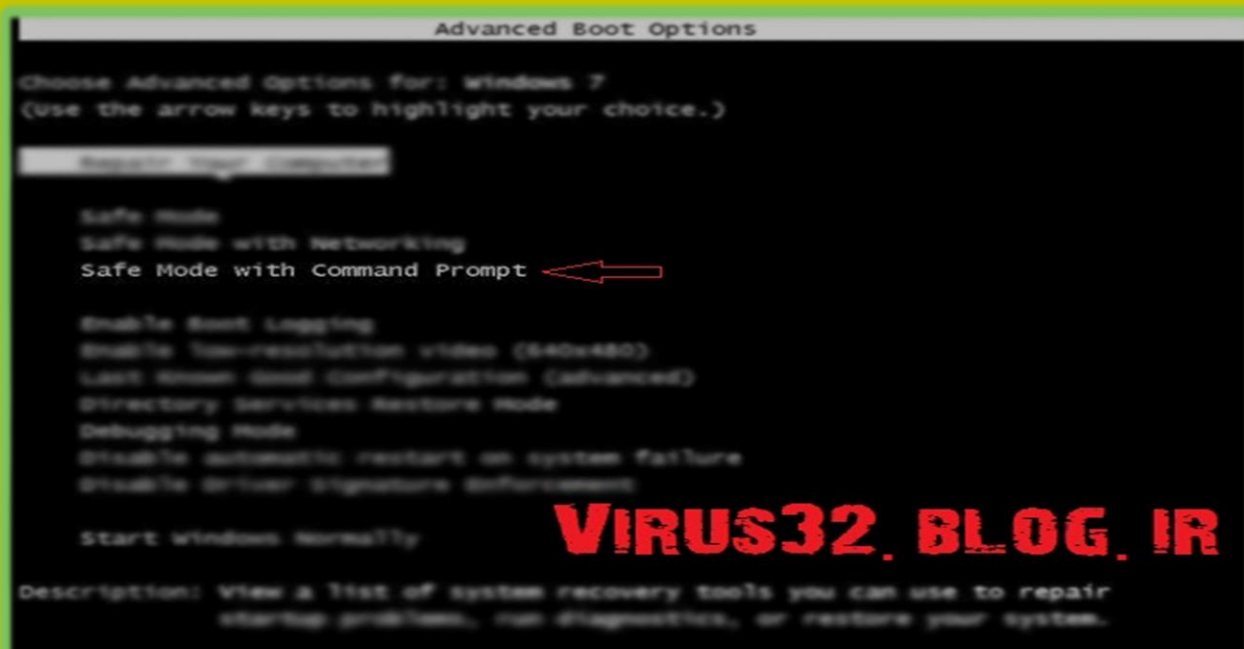
شاید مجبور شید چند بار سیستم رو به این صورت خاموش روشن کنید

۲- قصد ما فقط اینه که به قسمتی که برای تعمیر ویندوز گزینه هایی نمایش داده میشه برسیم  
یعنی اینجا:



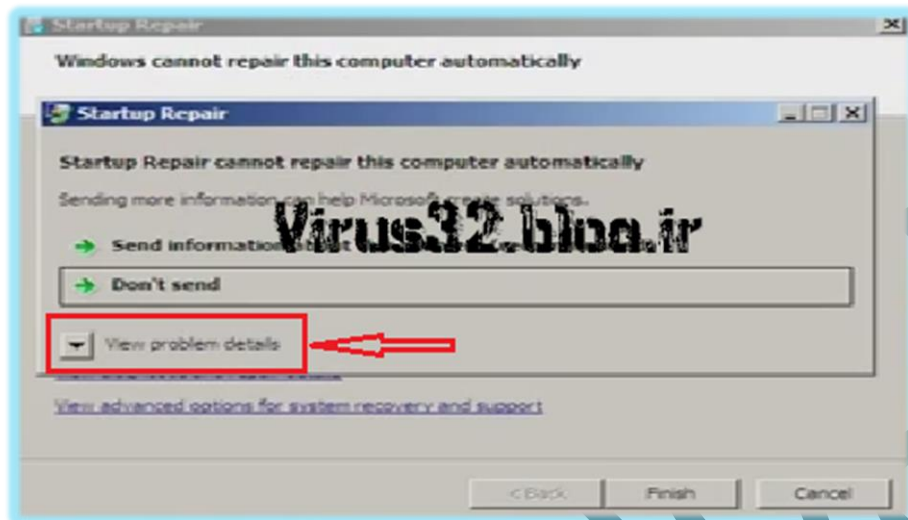
۳- خوب ما اینجا **Launch Startup Repair** رو انتخاب میکنیم.

قابل توجه! تو ویندوز اکس پی ، هنگام روشن شدن سیستم، کلید **F8** رو بزنید. و گزینه  
**Safe mode With Command Prompt** رو بزنید. میتونید وارد **CMD** بشید و هیچ  
دردسری دیگه ای نداره. و ادامه مراحل رو از شماره **۸** به بعد ادامه میدیم...



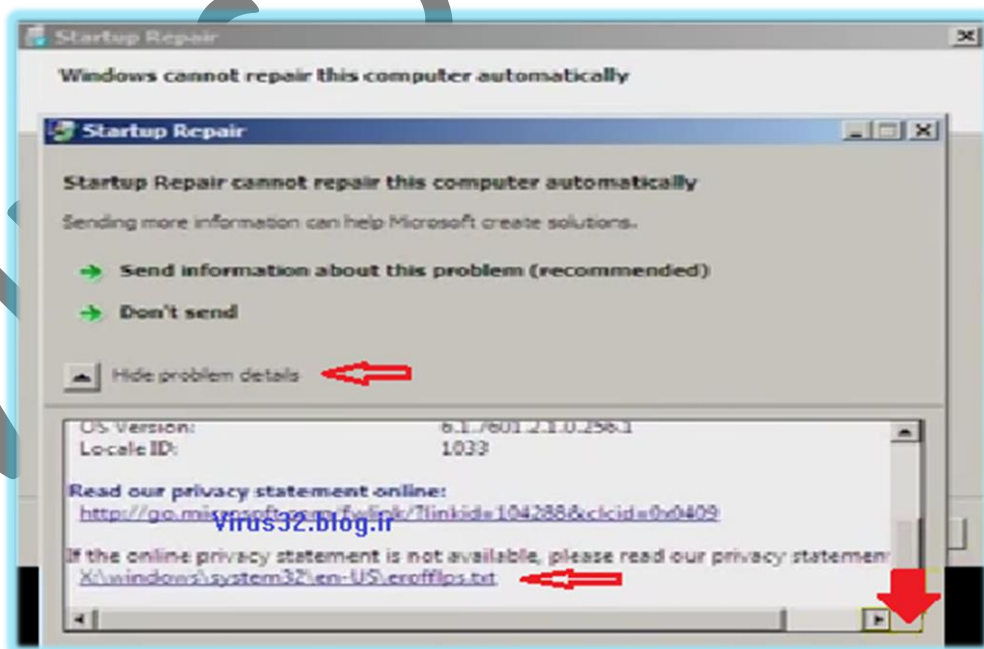
۴- منتظر میمونیم تا پنجره **Startup repair** با دو گزینه **send** و **no send** نمایش داده بشه

۵- در زیر این گزینه ها بر روی **View problem details** کلیک میکنیم تا جزئیات مشکل فرضی به وجود اومده رو به ما نشون بده.



۶- در لیست باز شده به انتهای لیست میریم که آخرین خط مربوط به **Privacy Statement** است. دقت کنید این خط به **txt** ختم میشه.

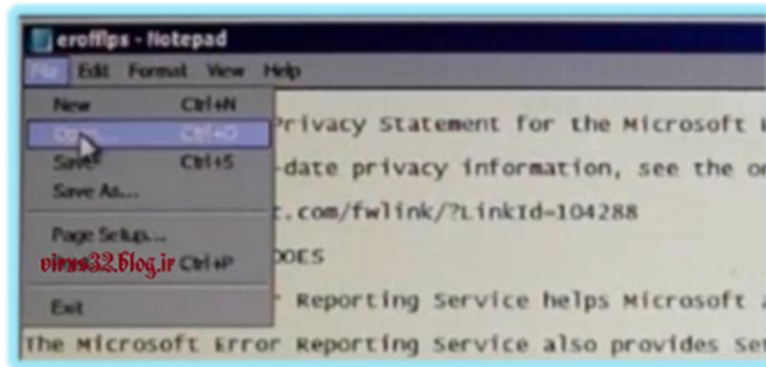
# در کل فرقی نمیکنه روی چه کلماتی کلیک میکنید مهم فرمت **txt** اختاره ، یعنی باید تو این لیست گزینه ای پیدا کنید که فرمت **txt** داشته باشه #



۷- خوب روش کلیک میکنیم و میبینید که فایل نوت پد اجرا میشه و یسری نوشته رو نمایش میده. که ما کاری به این نوشته ها نداریم.



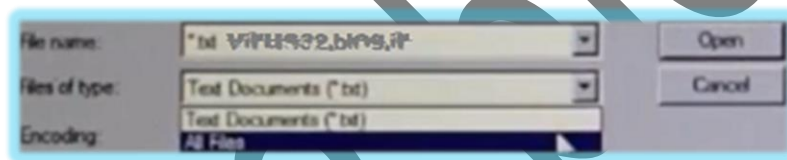
۸- از قسمت **File** بر روی **Open** کلیک میکنیم که وارد **My computer** میشه



۸- حالا ما باید به آدرس زیر بریم:

Computer -> Local Disk (C) -> Windows -> System 32

۹- از قسمت **File Of Type** گزینه **All File** رو انتخاب میکنیم.



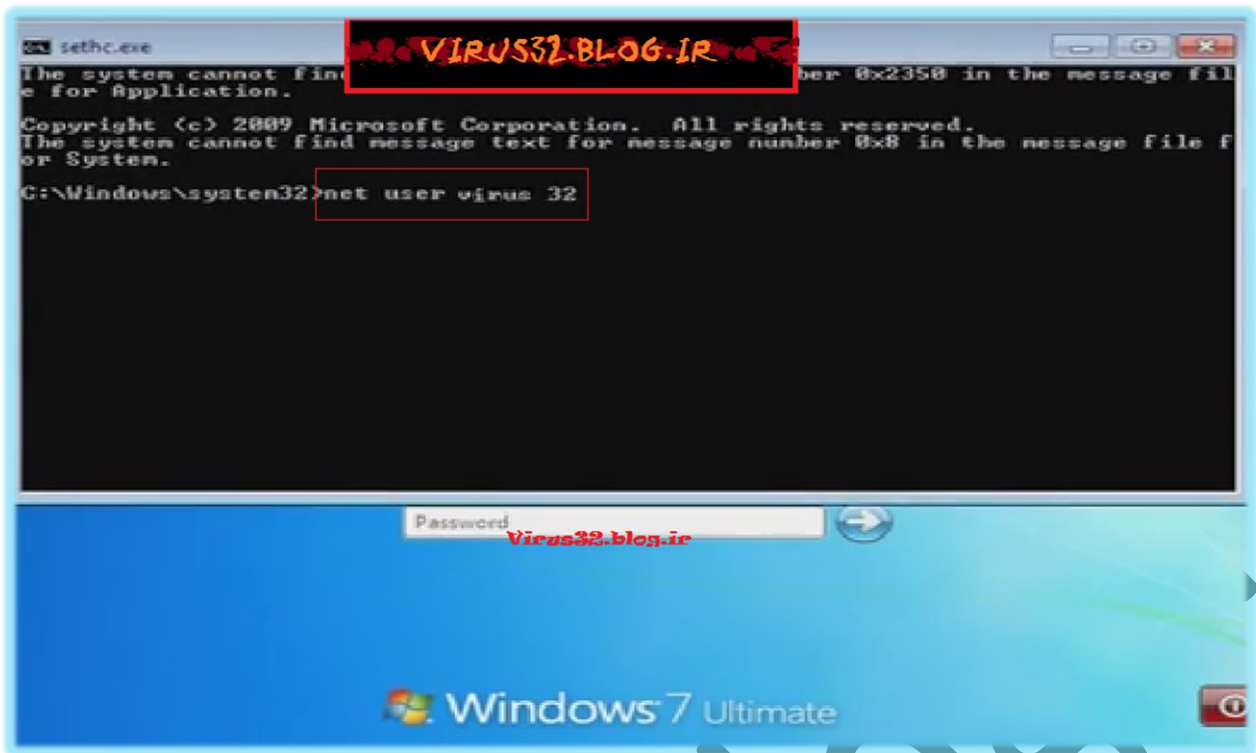
۱۰- سپس به دنبال فایل **Sethc.exe** میگردیم و اسمش رو تغییر میدیم ... مثلاً **Sethc1.exe** :

بعد برنامه **cmd.exe** رو در همون قسمت پیدا میکنیم یه کپی ازش میگیریم و اسم کپی این برنامه رو به **Sethc.exe** تغییر میدیم .

در اینجا کلاً یه بک آپ از فایل **Sethc.exe** و **cmd** گرفتیم و **cmd** رو به این فایل **Sethc.exe** تبدیل کردیم.

۱۱- حالا تموم پنجره هارو میبندیم و سیستم رو ریستارت میکنیم و به قسمتی که باید رمز عبور رو وارد کنیم میرسیم.

۱۲- در این قسمت کلید **Shift** رو بصورت متوالی ۵ بار فشار میدهیم که در این صورت برنامه **cmd** اجرا خواهد شد.



۱۳- حالا در سی ام دی دستور زیر رو وارد میکنیم

```
net user Virus 32
```

من اینجا برای نام کاربری که **Virus** بود رمز **۳۲** رو دادم

"دقت کنید بجای **Virus** باید نام اکانت سیستم رو وارد کنید و بجای **۳۲** رمز مورد نظر خودتون رو"

اگه نام اکانت سیستم رو هم نمیدونید مهم نیست کافیه ابتدا فقط دستور بالا رو بدون نام کاربری وارد کنید یعنی:

```
net user
```

۱۴- سپس سی ام دی رو میبندیم و در قسمت رمز، رمزی که انتخاب کردیم رو مینویسیم و وارد سیستم میشویم.

تمام!

**روش چهارم:** این روش توو همه ویندوز ها جواب میده. ولی نیاز به یک سیدی ویندوز دارید.

۱- اول سیدی ویندوز رو بزارید توو. بعد از اینکه بوت شد، صبر کنید تا درایوراتون شناسایی شه.

۲- بعد از اینکه صفحه زیر رو دیدید **Next** رو بزنید...

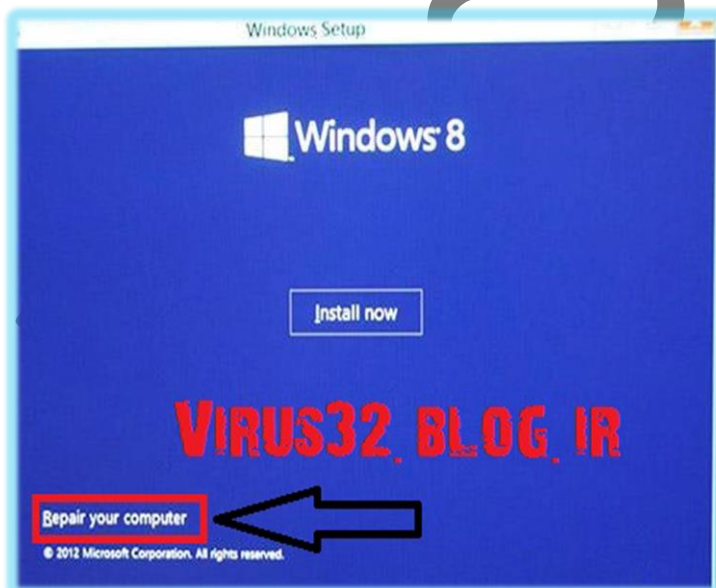


Windows 8

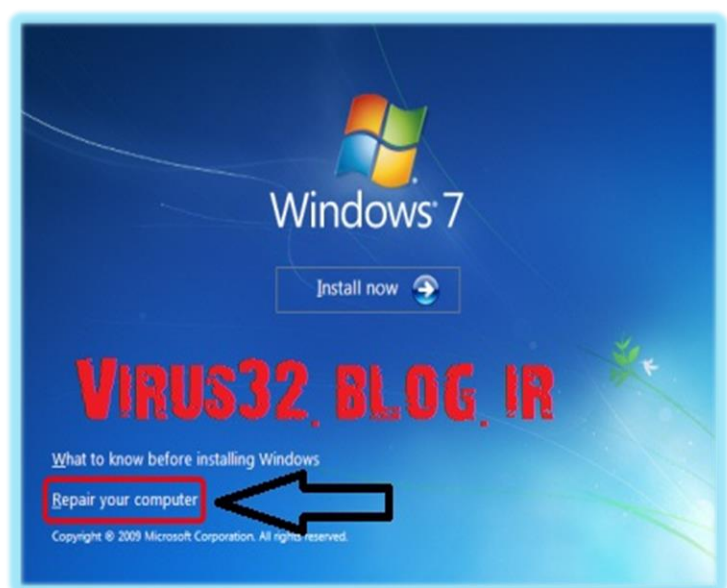


Windows 7

۳- در این قسمت میتونید کلید ترکیبی **Shift + F10** رو بزنید تا **CMD** ظاهر بشه یا روی گزینه **Repair your computer** کلیک کنید تا به منوی **Repair** وارد شوید...



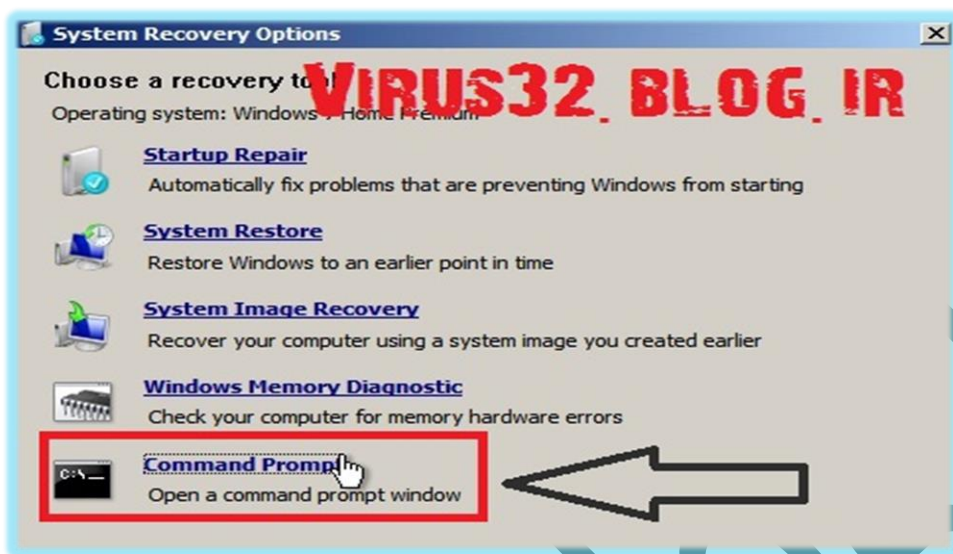
Windows 8



Windows 7



سپس در ویندوز ۷ روی گزینه **Command Prompt** کلیک کنید تا **CMD** ظاهر شه.

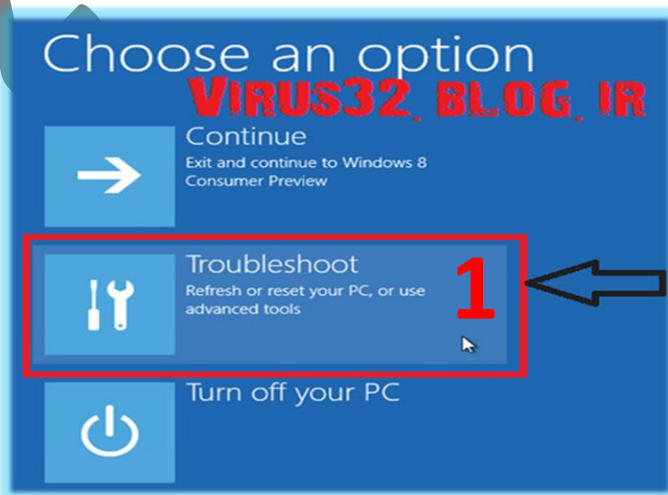


Windows 7

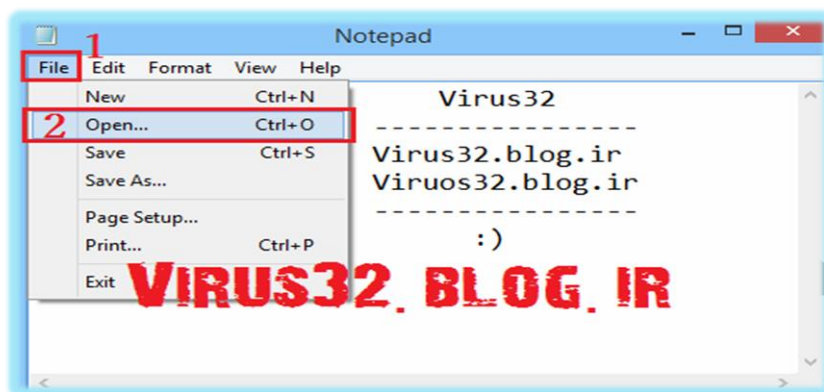
در ویندوز ۸ اول روی گزینه **Troubleshoot** کلیک و سپس روی **Command Prompt** کلیک کنید.



Windows 8



حالا **cmd** ظاهر شد. توو **cmd** تایپ کنید: **notepad** و اینتر کنید. می بینید که برنامه **Notepad.exe** اجرا شد، حالا در منوی **File** روی گزینه **Open** کلیک کنید.

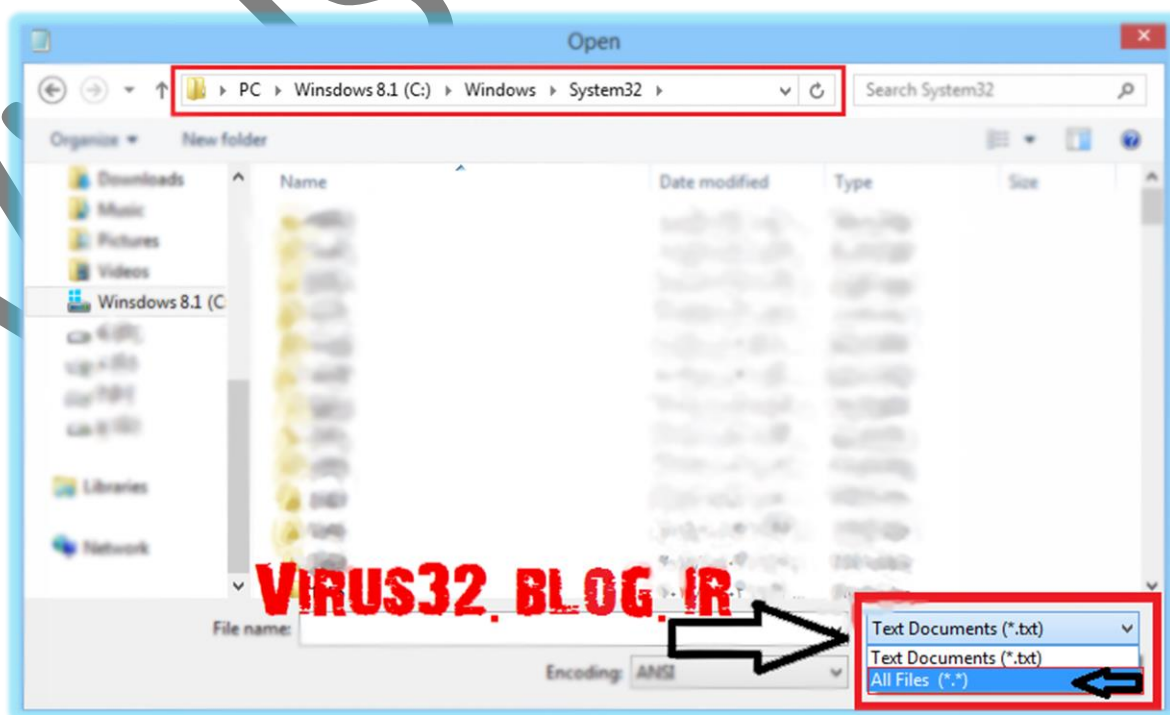


حالا باید مسیر زیر رو بریم. دقت کنید که احتمالاً نام درایو **C** اصلی شما در اینجا نام دیگه ای داره. همه ی درایو ها رو باز کنید تا درایو **C** اصلی خودتونو پیدا کنید. (نام درایو **C** سیستم من، نوع ویندوزم **Windows 8.1** هست.) بنابراین راحت میتونم پیدااش کنم. و سپس مسیر زیر رو برید:

( C:\Windows\System32 ) آدرس مرتب شده ش

Computer -> Local Disk (C) -> Windows -> System 32

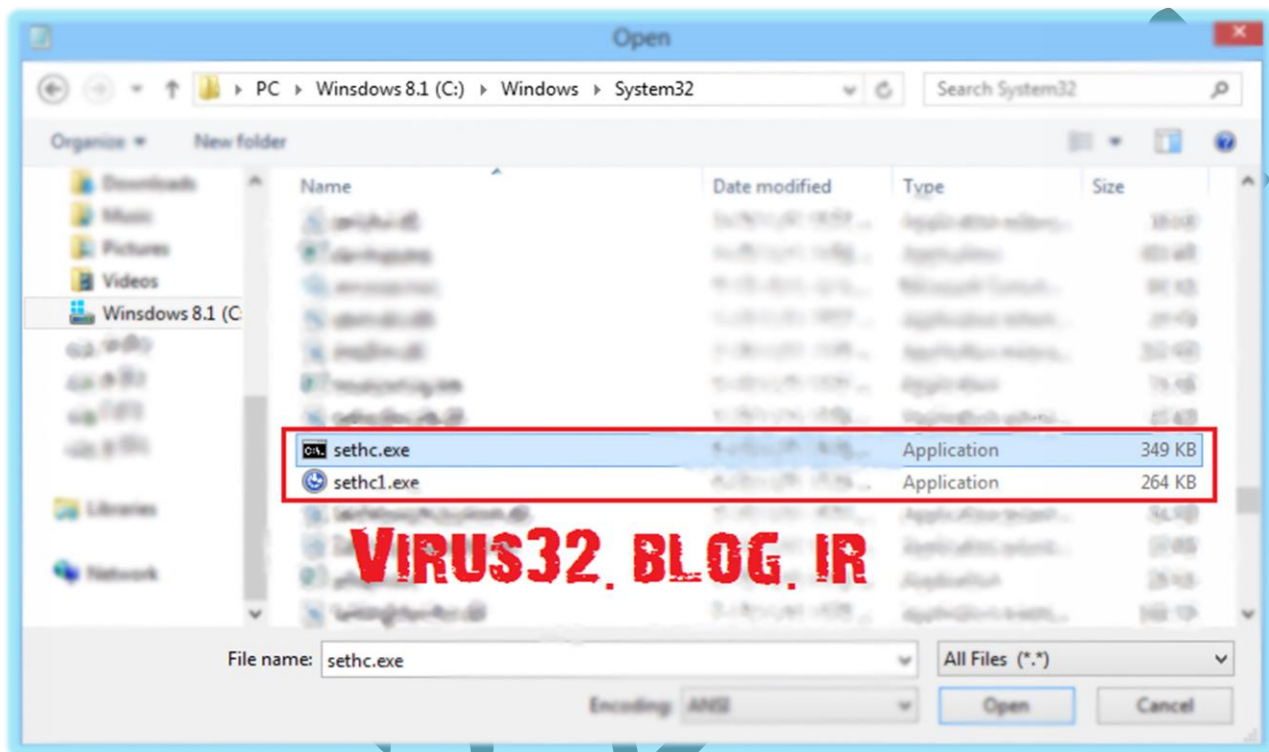
حالا از قسمت **File Of Type** گزینه **All File (\*.\*)** رو انتخاب کنید تا همه فایل ها را نشان دهد.



حالا بگردید دنبال فایلی به نام **sethc.exe** و اسمشو به **sethc1.exe** یا... تغییر بدید.

بعد بگردید دنبال فایلی به نام **cmd.exe** و ازش یه کپی بگیرید و همونجا پیست کنید یعنی بشه دوتا **cmd**. اسم **cmd** دومی رو از **cmd - Copy.exe** به **Sethc.exe** تغییر بدید.

کلید **F5** رو بزنید (**Refresh**)، میبینید...



حالا همه پنجره ها رو ببندید و سیستم رو ری استارت بدین!

وقتی سیستم بالا اومد و ازتون پسورد خواست. پنج بار کلید شیفت رو بزنید. میبینید که **CMD** ظاهر شد!؟!

حالا میریم توو کد نویسی! اگه پسورد رو فراموش کرده بودید و میخواید رمز یوزرتون رو عوض کنید این کد رو توو **CMD** بنویسید: `net user virus32 1234` به جای **virus32** اسم یوزرنیمتون (اکانت) و به جای **۱۲۳۴** پسورد جدیدتون رو وارد کنید. و اینتر کنید.

اگه نام اکانت سیستم رو هم نمیدونید مهم نیست کافیه ابتدا فقط دستور بالا رو بدون نام کاربری و پسورد وارد کنید یعنی: `net user`

این کد اسم یوزرتون رو بهتون نشون میده. یا اصلن اسم یوزر زیر یا کنار عکس یوزر نوشته (:

سپس در قسمت پسورد، رمزی که انتخاب کردیم رو مینویسیم و وارد سیستم میشیم. **تبریک**

**میگم بهتون:**

ولی اگه قصد **شیطونی**: دارید و نمیخواید کسی بفهمه که شما وارد سیستم شدید، این کد رو بزنی تا یه یوزر جدید براتون درست شه: `net user virus32 /add` بعد از اینکه **کارتون** تموم شد، باید ردپای خودتونو پاک کنید و یوزری که ساختید رو از بین ببرید. برای از بین بردن یوزر، از این کد استفاده می کنیم: `net user virus32 /delete`

تمام!

پایان

### انتقادات و پیشنهادات:



**Web**

[Virus32.blog.ir](http://Virus32.blog.ir)

[Virus32.blog.ir](http://Virus32.blog.ir)



**Yahoo mail**

**Virus32:**

[Virus\\_bad32@Yahoo.com](mailto:Virus_bad32@Yahoo.com)

**Virus32 Fake (Mozahem32):**

[Virus32Fake@Yahoo.com](mailto:Virus32Fake@Yahoo.com)



**Gmail**

**Virus32:**

[Virus.32bat@Gmail.com](mailto:Virus.32bat@Gmail.com)