

# به نام خدا


چه کار کنیم که **هک** نشویم؟

نویسنده: حمید رضا نیاز کار

سخنی با شما:

1. برای دانلود pdf های دیگر می توانید به آدرس [www.pcel-pdf.blogspot.com](http://www.pcel-pdf.blogspot.com) مراجعه فرمایید. که البته

هنوز کاملاً راه اندازی نشده...

2. انتقادی، پیشنهادی، فحشی، چیزی بود بگید مثلاً ما انتقاد پذیریم ...  [Hrn185@yahoo.com](mailto:Hrn185@yahoo.com)

3. راستی کپی هم نکنید حق خودم ضایع می شه... ولی کپی با ذکر نام نویسنده ایراد که نداره خوبم هست چون در

پیشرفت جامعه نقشی داشتیم این همون آرزوی منه...

4. اگر اشتباهی دستوری مشاهده کردید من پیشاپیش از شما عذر خواهی می کنم اشتباهات دستوری را با ما در میان

بگذارید تا در نسخه های بعدی آن را اصلاح کنیم.

همیشه خندون باشید.

## About this pdf:

Pages	6
Words	1,522
Characters (no spaces)	5,413
Characters (with spaces)	7,273
Paragraphs	54
Lines	126

## مقاله های دیگر ما:

View	لینک دانلود	نویسنده	کد	نام مقاله
	<a href="#">picofile</a> .1 <a href="#">4shared</a> .2	حمید رضا نیازکار	101	بازیابی و هک رمز عبور ورود به ویندوز
	<a href="#">picofile</a> .1 <a href="#">4shared</a> .2	حمید رضا نیازکار	102	مدیریت پیشرفته وبلاگ

برای محافظت از کامپیوتر در برابر ویروس ها و هکر ها راهکار هایی وجود دارد و با کمی رعایت می توان در محیط های سرشار از ویروس و هکر، مثلاً چت روم حضور پیدا کرد .

### راه های زیر خوراک هکر هاست :

1. چت روم
2. فیس بوک
3. سایت هاو وبلاگ های ناشناس
4. گروه های گوناگون forum موجود در اینترنت
5. vpn

### چت روم :

حتی حضور در محیط چت روم خطر سازه... من به شما توصیه می کنم که حتی الامکان از محیط چت روم برای چت با دوستان و آشنایان خود استفاده کنید . یک هکر تنها با ارتباط یک کلمه ای بین دو کامپیوتر از طریق محیط داس\* می تواند کامپیوتر فرد مقابل را خاموش یا restart کند اما مسئله این نیست و اگر هکر ماهر باشد می تواند با استفاده از نرم افزار هایی که از معرفی آن ها معذوریم به راحتی کامپیوتر شما را در دسترس می گیرد و فایل های شما را از کامپیوترتان سرقت کند و حافظه کامپیوترتان را پر از ویروس و اسب تروا یا تروجان کند. پس راه حل چیست ؟

- 1 - یک آنتی ویروس خوب بر روی کامپیوتر خود نصب کنید ، من Eset Nod 32 را به شما توصیه می کنم.
- 2 -آنتی ویروس خود را مدام به روز کنید برای این کار اگر به مشکل copyright برخورد کردید از update های offline استفاده کنید .
- 3 -درکنار آنتی ویروس خود ، آنتی ویروس دیگری نصب کنید که با یکدیگر سازگار و مکمل باشند مثلاً مکمل Eset Nod 32 ، Avast می باشد اگر مکمل آنتی ویروس خود را نمی دانید از یک آنتی تروجان استفاده کنید .
- 4 -فایروال ویندوز خود را همواره روشن بگذارید .



- 5- از دریافت فایل در محیط چت روم جداً خودداری کنید.
  - 6- از کلیک بر روی لینک های ناشناس خودداری کنید .
  - 7- هشدار های آنتی ویروس خود را جدی بگیرید !!!
  - 8- با کامپیوتر های عمومی چت نکنید یا حداقل بعد از sign out کردن با آی دی الکی و رمز الکی تلاش برای sign in کردن کنید.
  - 9- قبل از وارد کردن رمز کلید های ctrl + alt + s را فشار دهید اگر صفحه ای ظاهر نشد ادامه دهید در غیر اینصورت کامپیوتر شما توسط نرم افزار های جاسوسی کنترل می شود و رمز شما توسط صفحه کلید فاش می شود .
- مشکل های ناشی از هک شدن برای کسانی که از اینترنت dial up استفاده می کنند بسیار کمتر از کسانی است که از ADSL استفاده می کنند می باشد . متأسفانه در صورت نا آگاهی ممکن است طعمه ی باجگیر ها بشوید. فراموش نکنید که ساختن یک آی دی به اسم های دخترمانند کار بسیار ساده ای می باشد .

### فیس بوک :

فیس بوک ظاهراً محیطی امن و خوبی به نظر می رسد اما این طور نیست . یک هکر به راحتی می تواند با دانستن یک سری اطلاعات اولیه از هدف رمز آی دی او را به دست آورد و با دوستان فرد ارتباط برقرار کند و... مشکل بزرگ فیس بوک این است که ثبت آی دی در آن راحت تر از آب خوردن است . چاره چیست؟

- 1- ثبت نام آی دی خود را کامل کنید و آن را در حالت protection low رها نکنید یعنی شما باید سوال و جواب هنگام فراموشی رمز را وارد کنید .
- 2- ایمیلی جدید برای آی دی خود بسازید از ایمیل قبلی خود استفاده نکنید .
- 3- نا آشنایان را به عنوان دوست نپذیرید . (دوستی با آنان را رد کنید.)
- 4- اگر از ADSL استفاده می کنید کامپیوتر خود را در فیس بوک رها نکنید .
- 5- حتماً برای خارج شدن از اینترنت sign out کنید.

## 6- کوکی های کامپیوتر خود را مرتباً پاک کنید .

### سایت ها و وبلاگ های ناشناس :

این مورد خطر های کمتری نسبت به مورد های قبلی دارد اما تعداد زیادی روزانه از این طریق هک می شوند و خود نا آگاه باقی می مانند. گاهی اوقات سایت های (اکثراً ایرانی) اقدام به تشکیل خبرنامه می کنند و شما که از مطالب سایت لذت برده اید با تمایل دارید مطالب روزانه سایت را دریافت کنید. وبمستر با طراحی صفحه ای مانند log in یا هو شما را به آن صفحه می برد و از شما درخواست می کند که رمز و آی دی خود را وارد کنید این صفحه رمز و آیدی شما را برای هکر می فرستد در واقع شما گوشت را به دست گربه می دهید و رمز ایمیل خود را دو دستی به هکر تقدیم می کنید. این مورد اول از خطر هاست من چند مورد دیگر را ذکر می کنم. شما وارد وبلاگ یا سایتی می شوید که اصطلاحاً همه چیز تمام می باشد فرض می کنیم که سایت ترند های کامپیوتر ارائه می کند در میان صد ها ترند وبمستر شما را گیج می کند و به شما از طریق ترند می گوید که اگر مایل به هک کردن ایمیل مثلاً یا هو هستید راه حل از طریق خود سایت یا هو می باشد و شما باید رمز و آی دی خودتان را که باید از زمان ثبت نامش 2 ماه گذشته باشد همراه با آی دی هدف بفرستید برای فلان ایمیل و یا هو هنگ می کند و رمز را برای آی دی شما می فرستد. من خودم بارها و بارها این مطلب را در وبلاگ های مختلف دیده ام این حماقت تمام است که ما فکر کنیم یا هو به این راحتی ها هک می شود اکثر اوقات ایمیلی که قرار است برای آن اطلاعات را بفرستید با کمی زرنگی هکر آدرسی است که اصلاً شک نمی کنید مثلاً هکر کلمه register را در ایمیل خود دارد تا شما را همراه کنده این مورد دوم و مورد سوم بدون هیچ آگاهی انجام می شود شما وارد سایتی می شوید سایت کوکی های شما را از کامپیوتر سرقت می کند و کوکی ها هم که ما شالاه همی رمزها و زندگی ما را در خود جای داده اند این مورد سوم و مورد چهارم هم این است که شما مانع مورد قبلی وارد آدرسی شوید هکر کد های را در سایت خود به همراه یک ویروس جای داده است این کدها ویروس را بر روی کامپیوتر شما بدون آگاهی خودتان نصب می کند و آنرا گسترش می دهد اگر به جای ویروس هکر از تروجان استفاده کند رمز های شما نیز لو می رود و مورد پنجم بر می گردد به دانلود از روی نا آگاهی ... راه حل برای موارد بالا چیست ؟

1. هیچ جای اینترنت رمز و آی دی ایمیل خود را وارد نکنید .

2. از صفحه log in یا هو و یا هر سایت دیگر اطمینان کامل پیدا کنید .

3. به ایمیل هایی که درون آنان لینک های نا شناس قرار دارد توجهی نکنید چون همین لینک عامل هک است.
4. وسوسه هک دیگری را نداشته باشید تا گول نخورید بدانید که هک کردن آی دی کاری به این راحتی نیست.
5. کوکی های خود را مدام پاک کنید .
6. یک نرم افزار دانلود نصب کنید (ضروری) مثلاً internet download manager
7. از پاک بودن فایل های دانلودی صحت کامل داشته باشید .
8. از سایت های leech گمنام استفاده نکنید.

### گروه های گوناگون forum موجود در اینترنت :

این گروه ها از ناآگاهی شما استفاده می کنند و شما را هک می کنند برای در امان ماندن هر مطلب این گروه ها را امتحان و یا تجربه نکنید و حرف های آنان را باور نکنید از توضیح بیشتر معذورم .

### Vpn :

این vpn ها شاید در ظاهر فقط به شما خدمات ارائه کنند اما بعضی از آنان کوکی های شما را به سرقت می برند می دانید که vpn مخفف virtual private network می باشد یعنی شبکه مجازی خصوصی شما با ارتباط از طریق vpn به این شبکه متصل می شوید پس دزدی اطلاعات امری امکان پذیر و راحت می باشد. راه حل اطمینان کامل از صحیح بودن خدمات vpn می باشد.

### مهندسی اجتماعی : (راستش رو بخواهید من نمی خواستم در مورد این روش چیزی نویسم اما برای کامل شدن این مقاله مجبورم ...)

این روش بین هکر های بی سواد رایج است. در این روش ، هکر به وبمستر ها یا وبلاگ نویس ها میگوید که از وبلاگ شما خوشش آمده و قصد همکاری با شما را دارد . او ایمیل خود را برای شما می نویسد و می گوید که اگر خواستید به او ایمیل بزنید، هکر برای اطمینان که شما به او ایمیل می زنید با لفظی دخترانه پیغام بالا را می نویسد و آی دی که معمولاً در آن از اسم های مونث استفاده می کند گول این هکر ها را نخورید که پس از ایمیل شما آنان از شما رمز و نام کاربری را می خواهند و وبلاگ شما را به دست می گیرند.