

بسم الله الرحمن الرحيم



پلیس فتا، سایه سار امنیت در فضای مجازی

[www.cyberpolice.ir](http://www.cyberpolice.ir)



## ۱۶ safety tips to prevent intrusion into computer



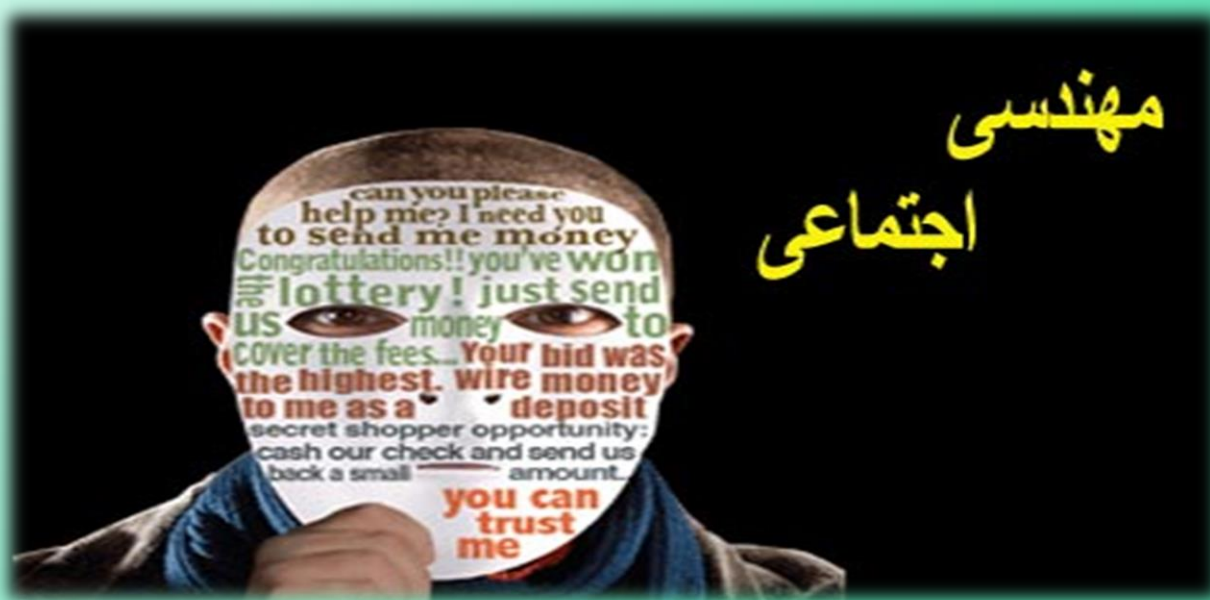
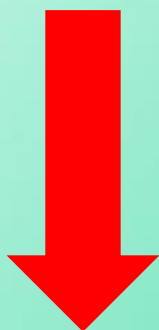
۱۶ نکته

امنیتی برای جلوگیری از نفوذ به رایانه





متداول ترین روش هکرها برای نفوذ به سیستم های رایانه ای مهندسی اجتماعی می باشد . روش مهندسی اجتماعی یکی از روشهای سخت و در عین حال آسان است، که اگر شما اطلاعاتتان را کمی بالا ببرید استفاده از این روش حتی برای حرفه ای ترین هکرها نیز دشوار خواهد شد.



مهندسی  
اجتماعی



کاربران در انتخاب گذر وازه های خود دقت کافی و لازم را به خرج دهند. بعضی افراد **شماره تلفن، شماره شناسنامه، تاریخ تولد،** و ... را برای پسورد خود انتخاب می کنند. زیرا به قول خودشان پسوردها را زود فراموش می کنند. همیشه در پسورد خود از **اعداد و کلیدهای** مثل **Space** استفاده کنید. و همچنین پسورد خود را با طول زیاد انتخاب کنید. این روش امکان هک شدن شما را کاهش می دهد.





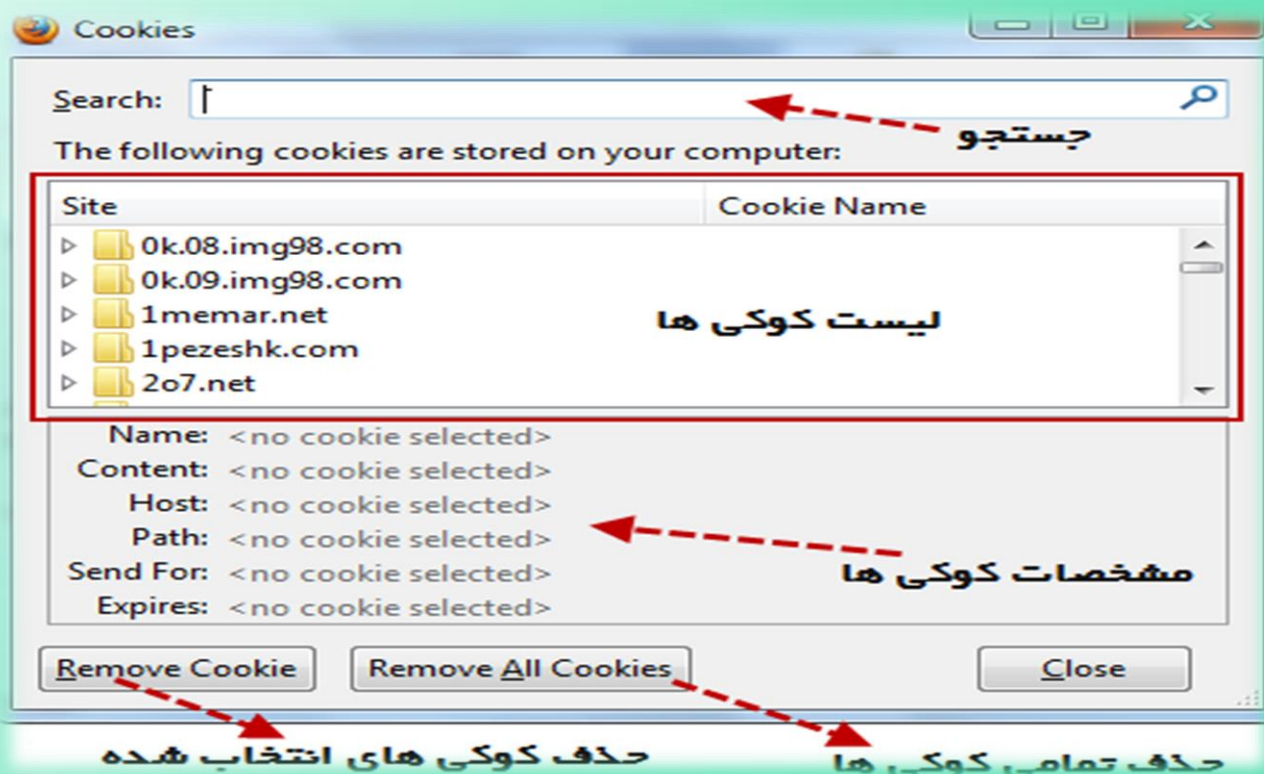


یکی از روشهایی که افراد فرصت طلب هنوز از آن استفاده می کنند دزدیدن پسورد از روی حرکت دستهای شماست. هنگامی که پسوردتان را وارد می کنید مراقب چشمهای اطراف خود باشید.



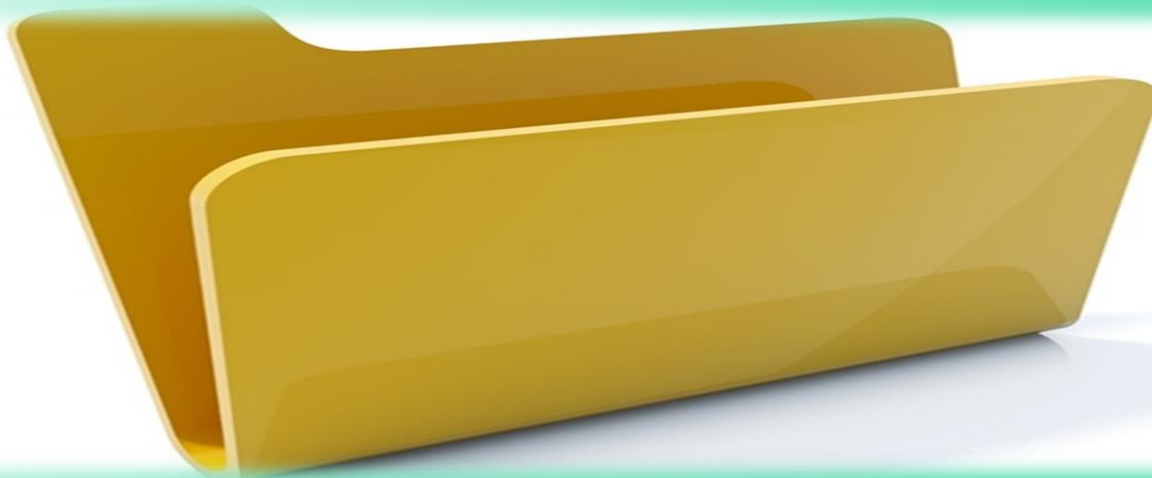
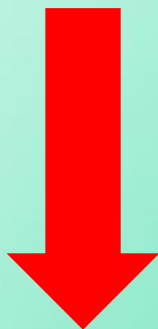


**Cookie** مرورگرها گزینه دیگری است که مورد توجه هکرها می باشد . کوکی ها اطلاعات حیاتی را نگه می دارند. البته به صورت کد شده، ولی افراد حرفه ای میتوانند آن را از حالت کد شده در آورند تا اطلاعات مفیدی بدهد.



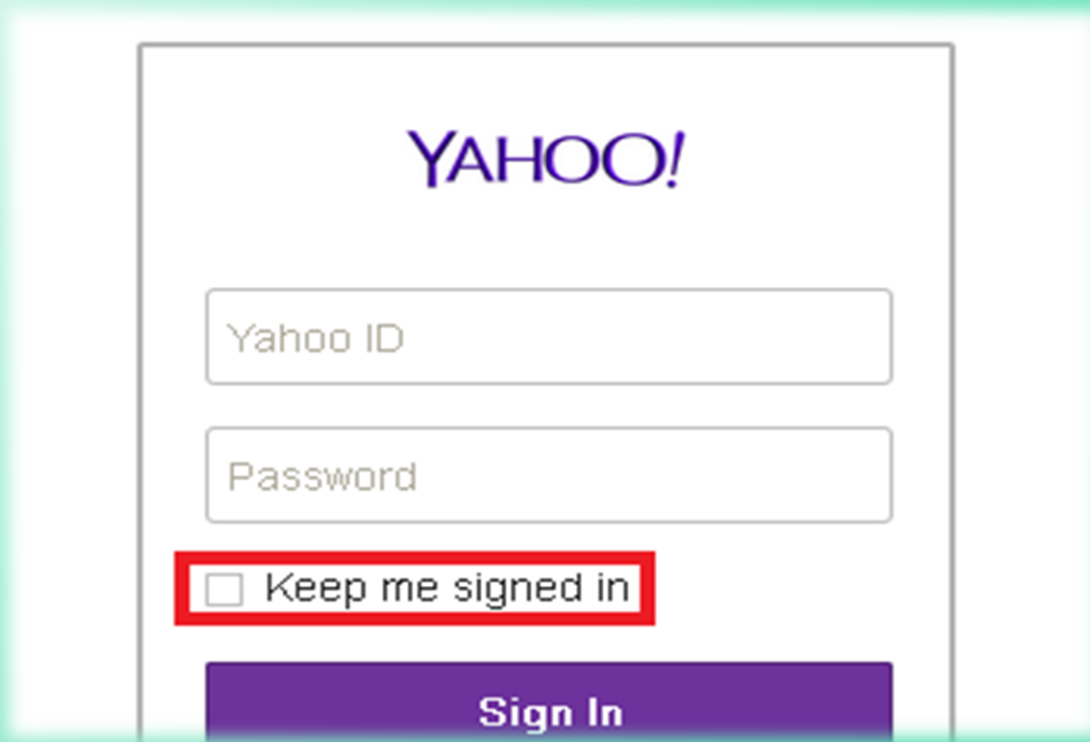
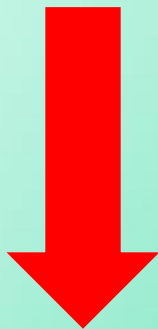


گذرواژه هایی خود را بصورت تکس در فایل ذخیره نکنید زیرا  
در صورت نفوذ به سیستم شما حساب هاب کاربری شما نیز  
مورد دستبرد قرار می گیرد .





هنگام استفاده از ایمیل ، تیک گزینه **Remember** را برداشته و حتما هنگام خارج شدن از گزینه **Logout** استفاده کنید.



YAHOO!

Yahoo ID

Password

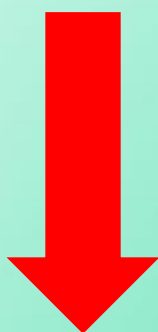
☐ Keep me signed in

Sign In





نفوذ گران با بهره گیری از بستر ایمیل اقدام به ارسال فایل های آلوده به کاربران می نمایند لذا به هیچ عنوان بر روی لینک های ارسالی توسط افراد ناشناس کلیک نکنید .





هنگام دانلود کردن برنامه ها سعی کنید از سایت های معتبر، برنامه هایتان را دانلود کنید. و اگر هم ممکن نبود حتما از سایت موردنظر اطمینان پیدا کنید و بعد از دانلود فایل ها را ویروس یابی کنید.



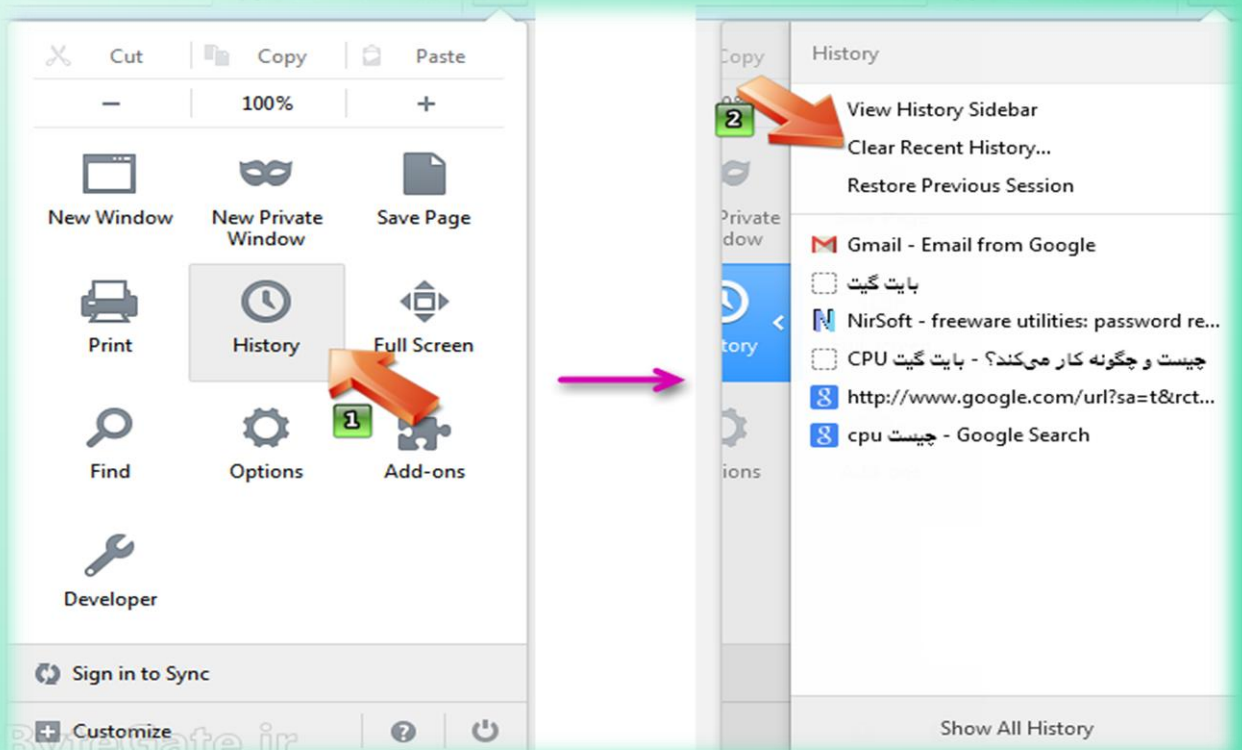


در وب گردی مراقب سایت های آلوده باشید زیرا برخی  
سایت ها بدون اطلاع کاربر اقدام به نصب پلاگین های  
مخرب می نمایند .



۹

اگر نیازی به اطلاعات History ندارید هر از چند گاهی آن را پاک کنید.







کیلاگر (Keylogger) برنامه های جاسوسی هستند که می توانند اطلاعات شما را ضبط و ثبت کنند. راههای ورودی کیلاگرها را با نصب آنتی ویروس مناسب و فایروال مسدود نماید.





از رایانه های عمومی برای انجام امورات مهم خود مانند  
عملیات بانکی و ... استفاده ننمایید .



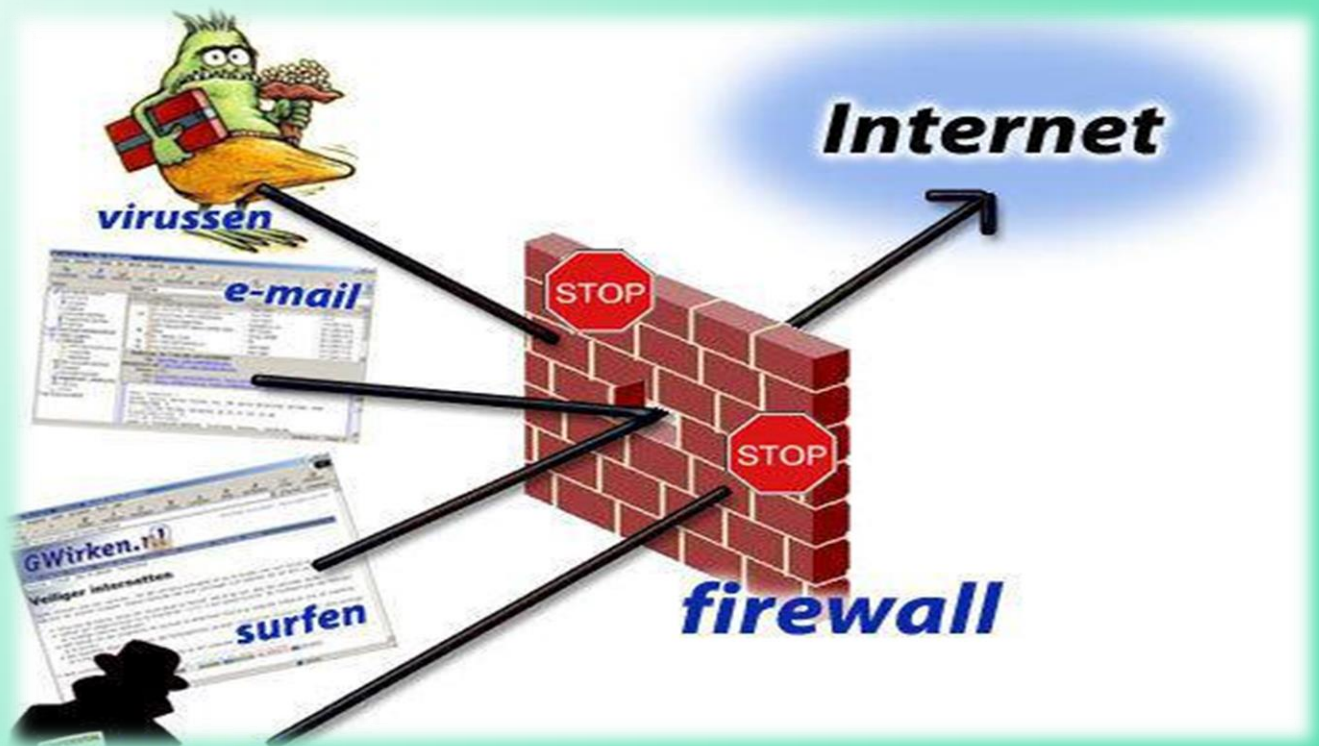


در زمان استفاده از مراکز ارائه دهنده اینترنت ( نت سراها )  
حتما به نکات امنیتی توجه داشته باشید و از ذخیره اطلاعات  
خود در این سیستم ها جدا پرهیزید .





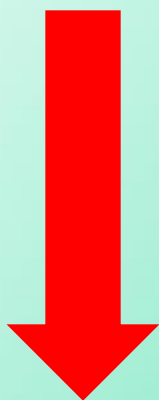
سیستم های رایانه ای خود را مجهز به آنتی ویروس و فایروال  
بروز نمایید این دو برنامه سد دفاعی شما در برابر تهدیدات  
در فضای وب می باشند.







سیستم عامل و نرم افزارهای منصوبه بر روی سیستم خود را همیشه بروز نگه دارید .



⋮ Configuring Windows updates  
87% complete  
Do not turn off your computer.

۱۵

بیشتر حملات سایبری امروزه از طریق مرورگرهای وب هستند. مرورگر خود را همیشه به روز نگه دارید.





هنگام ثبت نام کردن در سایتهایی مانند یاهو و گوگل و ...  
سوالی مبنی بر این که اگر روزی پسورد خود را فراموش  
کردید و یا تاریخ تولد را از شما سوال میکند. این  
مشخصات را به دقت به خاطر بسپارید تا در موقع ضروری  
بتوانید از آنها استفاده کنید.



YAHOO!

With a Yahoo! Account, get free email and other leading web services.

Sign in with an ID you already have



Can't access my account

Name  First Name  Last Name **1**  
 Gender  - Select One - **2**  
 Birthday  - Select Month -  Day  Year **3**  
 Country  Iran **4**

Select an ID and password

Yahoo! ID and Email  @ yahoo.com  **5**  
 Password  Password Strength  **6**  
 Re-type Password  **7**

In case you forget your ID or password...

Alternate Email (optional)  **8**  
 Secret Question 1  - Select One - **9**  
 Your Answer  **10**  
 Secret Question 2  - Select One - **10**  
 Your Answer