مقابله با تروریسم اسلامی در فضای مجازی

راهنمایی برای ارتقای امنیت ارتباطات کامپیوتری

فروردین 1388

تالیف و گردآوری: بهزاد جواهری

فهرست مطالب

معرفی

جمهوری اسلامی، دشمن اینترنت و کاربران آن

روز ۱۲ مارس ۲۲ برابر با ۲۲ اسفند 1387، گزارشگران بدون مرز به مناسبت روز جهانی مبارزه با سانسور لیست "کشورهای دشمن اینترنت" را منتشر نمود. این گزارش شامل وضعیت آزادی بیان در دنیای مجازی و سانسور اینترنت در ۲۱ کشور جهان می باشد. بر اساس این گزارش ایران در صدر کشورهای سرکوبگر آزادی بیان و دشمن اینترنت قرار دارد.

قوانین قرون وسطایی رژیم اسلامی مجازاتهایی را برای استفاده کنندگان از اینترنت در نظر گرفته است. بر اساس ماده 13 قانون "تشدید مجازات اخلال در امنیت روانی" مصوب ۱۲ تیر ماه 1387 دایر کردن وبلاگ و وبسایت مروج "فساد و فحشا"، مصداق الحاد و مجازاتی برابر جرایمی مانند "راهزنی، سرقت مسلحانه، تجاوز به عنف، تشکیل خانه فساد و فحشا" دارد. بر اساس همین ماده قانونی اشخاصی که وبلاگ و سایت های مروج "فساد و فحشا و الحاد" را اداره نمایند به عنوان "محارب و مفسد فی الارض" شناخته می شوند، جرمی که مجازات آن اعدام می باشد!

بازداشت وبلاگ نویسان و فعالین اجتماعی، تحقیر، شکنجه و در مواردی قتل بازداشت شدگان در راستای ایجاد فضای رعب و وحشت و نهادینه کردن تروریسم اسلامی در فضای مجازی می باشد. برخورد رژیم اسلامی به اینترنت و دنیای مجازی چالشی بزرگ را در مقابل کاربران اینترنتی قرار داده است. در مقابل سخت گیریهای اعمال شده کاربران دنیای مجازی راهی جز مقابله با ترفندهای رژیم و و سعی در حفاظت خویش در مقابل تهدیدهای موجود ندارند.

شاید از خود بپرسید که شما کار غیر قانونی انجام نمی دهید، بنابراین چه دلیلی برای رعایت مسایل امنیتی در اینترنت وجود دارد. مجموعه ای از قوانین که در چهارچوب قانون مجازات اسلامی تحت عنوان جرایم ضد امنیت داخلی و خارجی کشور "قوانین امنیتی" هستند به رژیم اختیارات وسیعی برای سرکوب هر نوع فعالیت مسالمت آمیزی را می دهد که به نحوی انتقاد از سیاست هایش می داند. اگر جواب شما به هر یک از سوالات زیر مثبت باشد به شما پیشنهاد می کنیم که امنیت خود را جدی بگیرید:

آیا از طریق اینترنت نامه ای به دوست خویش در خارج کشور فرستاده اید؟ آیا به کسی ای میل داده ید؟ آیا با کسی چت کرده اید؟ آیا خاطرات خود یا مطالب مهم دیگری را در کامپیوترتان نگاهداری می کنید؟ آیا فعال سیاسی یا اجتماعی هستید و با فعالین دیگر در ارتباط هستید؟ آیا از تلفن موبایل برای ارتباطات خود استفاده می کنید؟ اگر هر کدام از این کار ها را انجام میدهید بالقوه در معرض دسترس پلیس هستید و برای جلوگیری از دسترسی پلیس به این اطلاعات باید اقدامات پیشگیرانه ای را انجام دهید.

معمولا متخصصین کامپیوتر امنیت را مقوله ای بسیار تخصصی و خارج از محدوده فهم کاربران متوسط کامپیوتر وانمود میکنند. به همین دلیل بسیاری از کاربران اینترنتی اصولا از خیر "پیشگیری" از آلودگی پلیس میگذرند و به اصطلاح با اتکا به "انشاالله چیزی نمیشود" خود و دیگران را در معرض خطر و نفوذ پلیس قرار میدهند.

اینجا هدف ما این است که با زبانی واضح شما را با مفاهیم و اقدامات ابتدایی که امنیت استفاده از کامپیوتر، اینترنت و تلفن موبایل را بالا میبرد آشنا نماییم. مخاطب ما در این بحث ها فعالین سیاسی و اجتماعی است. جنبه ها، زوایا و مفاهیم دیگر در امنیت کامپیوتر اینجا مورد نظر نیستند.

فصل اول: هک و هکر

منظور از هک چیست؟

واژه هک به نفوذ در یک کامپیوتر یا شبکه ای از کامپیوترها گفته می شود و هکر کسی است که هک میکند! هکر پس از نفوذ به یک کامپیوتر می تواند به اطلاعات موجود در آن کامپیوتر منجمله نام های کاربری (username) ، پسورد ها، فایل ها و اسناد و مدارک شخص موجد روی کامپیوتر دسترسی پیدا کرد. در بعضی مواقع حتی می توان کامپیوتری که هک شده است را از راه دور کنترل کرد. درجه سختی هک کردن یک کامپیوتر بستگی به سیستم عامل و سد های دفاعی آن دارد. بطور کلی هک کردن کامپیوتر هائی که از سیستم عامل ویندوز (Windows) استفاده میکنند از کامپیوترهائی که از سیستم عامل یونیکس یا لینوکس استفاده میکنند ساده تر است. هک کردن یک سیستم کامپیوتری ویندوز بدون سد دفاعی کار بسیار ساده ای است که معمولا هر هکر تازه کاری میتواند انجام دهد. نفوذ به کامپیوتری که سد دفاعی داشته باشد کار آسانی نیست، وقت و تجربه بسیاری می خواهد و در بسیاری از مواقع تنها برنامه نویس های کامپیوتری قادر به انجام آن هستند.

هکر کیست ؟

هکر به شخصی گفته می شود که بتواند بطور غیر مجاز به یک یا مجموعه ای از کامپیوترهای دیگر دسترسی پیدا کند. بطور کلی می توان هکرها را به ۳ دسته تقسیم نمود:

1. هکر کلاه سفید: هکر کلاه سفید، در زبان عامیانه، به هکرهای "خودی" گفته می شود. اینها با نفوذ به شبکه های کامپیوتری سعی در آشکار کردن و رفع حفره های امنیتی دارند و قصد استفاده و ضربه زدن ندارند. از این نوع هکرها با نام "هکرهای خوب" نام برده می شود و امروزه در بسیاری از دانشگاههای اروپایی و آمریکایی افرادی در این زمینه آموزش دیده و به استخدام در شرکتهایی که خدمات امنیتی ارائه می کنند، در می آیند.
2. هکر کلاه سیاه: هکر کلاه سیاه به هکری گفته می شوند که با نفوذ به سیستم قصد استفاده از اطلاعات آن و ضربه زدن به شبکه را دارد.
3. فریکرها: فریکرها مانند هکرهای کلاه سیاه هستند با این تفاوت که فریکرها به قصد استفاده مجانی از تلفن و همچنین استراق سمع به خطوط تلفن نفوذ می کنند

آیا هکرها میتواند به کامپیوتر من دسترسی پیدا کند؟

جواب به این سوال می تواند مثبت و یا منفی نیز باشد. یک هکر با استفاده از ضعف امنیتی در کامپیوتر شما میتواند به آن نفوذ کند. در نتیجه اگر مسایل امنیتی را در استفاده از کامپیوتر تان را رعایت کرده باشید احتمال این نفوذ را بشدت کم میکنید. تنها راه پیشگیری از دسترسی هکرها به کامپیوتر و ارتباطات کامپیوتری شما بالا بردن سطح آگاهی در زمینه امنیت رایانه ای و اجرای توصیه های امنیتی است.

هکرها چگونه می توانند کامپیوتر من را هک کنند؟

هکرها برای نفوذ به یک کامپیوتر از روش ها و ابزارهای متفاوتی استفاده می کنند. کلا هک کردن میتواند شامل مراحل زیر باشد:

1. یافتن حفره امنیتی
2. نفوذ به سیستم با استفاده از حفره یافت شده
3. نصب برنامه (کرم ها و ویروس ها) ی جاسوس
4. بدست آوردن پسوردها و دسترسی کامل به کامپیوتر شما

دسته بندی آلودگیهای کامپیوتری

می توان آلودگی‌های کامپیوتر را این گونه دسته‌بندی کرد:

1- ویروس ها: یک ویروس برنامه ای بسیار کوچک است که خود را به برنامه های حقیقی و بزرگتر وصل میکند و به اصطلاح روی آنها سوار می‌شود و با نصب یا اجرای برنامه اصلی خود را وارد سیستم کامپیوتر می کند و شروع به کپی برداری از خود می شوند. پس از ورود به ویروسها شروع به تخریب سیستم و یا انجام کاری که برایش تعریف شده میکند. مثلا پیام فرستادن به کامپیوتر های دیگر، فرستادن مخفیانه اطلاعات به پلیس یا هکر طراح آن و یا ...

اسب تروجان (Trojan Horse) یکی از مخرب ترین برنامه ها می باشد که شروع به پاک کردن اطلاعات و یا غیر فعال کردن عوامل امنیتی دستگاه می کند تا هکر بتواند به راحتی فعالیتهای شما را کنترل کند. اسبهای تروجان قادر به ضبط فعالیتهای شما می باشند. اسبهای تروجان مانند ویروسها قادر به کپی برداری از خود نیستند اما می توانند به وسیله ویروسها به کامپیوترها وارد شوند. بعضی از تروجان ها توانایی سرویس دهی برای هکرها را نیز دارند; یعنی اگر تروجانی در کامپیوتری اجرا شود فرستنده آن تروجان میتواند کامپیوتر قربانی را با استفاده از کامپیوتر خود و از راه دور کنترل کند و عملیاتی بر روی کامپیوتر (مانند: کنترل Webcam و صدای کامپیوتر، حذف فایل , مشاهده درایوها، فرمت کردن درایوها و ...) انجام دهد. انواع مختلف تروجانها وجود دارند که ما به مهمترین نوع آن می پردازیم.

کی‌لاگر (Keylogger)- به اسب تروجانی گفته می‌شود که قادر است هرچه شما روی کامپیوتر تایپ میکنید را ضبط کند و این اطلاعات را برای جاسوس بفرستد. بدین ترتیب تمامی فعالیتهای شما روی کامپوتر از جمله آدرس ایمیل و پسورد آن و وبسایتهایی را که بازدید کرده اید، ای میل ها و چت ها و غیره را در اختیار پلیس قرار دهد. ویروس ها همچنین از راههای دیگری می توانند وارد کامپیوتر شما شود، منجمله:

- از طریق دسترسی فیزیکی به کامپیوتر شما و نصب مستقیم این نوع نرم افزارها.
- از طریق باز کردن ضمیمه های ایمیل، به هیچ وجه ضمیمه های ایمیل را با پسوند exe. باز نکنید. توجه داشته باشید که فایل های مایکروسافت ورد میتوانند حامل ویروس باشند. **از باز کردن ضمیمه ایمیل از افرادی که آنها را نمیشناسید خود داری کنید**.
- از طریق استفاده از وبسایتهایی که این ویروس ها در آن جا سازی شده اند .صفحاتی که عکس یا عکسهای آنها نمایان نمی شود را Refresh نکنید ، چون این یکی از روشهای آلوده سازی کامپیوتر قربانی به ویروس یا تروجان است و برای دیدن عکس مذکور روی آن کلیک راست بزنید و سپس گزینه Show Picture را بزنید . ممکن است سایتی حتی قسمتهای دیگرش نیز به درستی باز نشده باشد در این صورت نیز Refresh نکنید و آدرس آن سایت را در یک صفحه جدید وارد کنید
- از طریق نصب برنامه های آلوده
- در هنگام چت با دوستان خویش و دریافت فایلهائی که آلوده هستند.

2- کرم‌ها (Worms): کرم برنامه یا ویروسی است که از شبکه‌های کامپیوتر برای تکثیر خود استفاده می‌کند. یک کرم کل شبکه را برای ماشین دیگری که نقطه ضعف امنیتی مشخصی دارند جست و جو می کند و با یافتن این نقطه ضعف، خود را در کامپیوتر جدید کپی می کند و با راه یافتن کرم به ماشین جدید چرخه دوباره تکرار می شود و کرم دوباره از این جا در ماشین های جدید کپی می‌شود. ویروسها معمولا یک کامپیوتر منفرد را آلوده می کنند و سعی نمی کنند به کامپیوتر دیگری راه پیدا کنند، در صورتی که کرمها با آلوده کردن یک کامپیوتر سعی می کنند که با استفاده از مثلا آدرس های ای میلی یا لیست کنتاکت هائی که روی آن کامپیوتر هست خود را به کامپیوترهای دیگر منتقل کنند. به علت اینکه این انتقال بین کامپیوترها به طور خودکار انجام می پذیرد سرعت گسترش آنها بسیار سریعتر از ویروسها است. کرم در حافظه اصلی کامپیوتر (RAM) مستقر می شود و شروع به تکثیر خود می کند که موجب کند شدن سیستم می گردد. برای جلوگیری از آلودگی به کرم هیچ فایل پیوست (attachment) غیر منتظره ای را درایمیل های خود باز نکنید (بخصوص آنهایی را که شامل پیغامهایی فریبنده مانند I LOVE YOU وجود دارد)، هر چند آنها از منابع مطمئنی برای شما ارسال شده باشند.

برای فرستنده ایمیلی بفرستید و از او سئوال کنید او واقعاً چنین فایلی برای شما فرستاده است یا نه؟ همچنین برنامه Outlook Express از شرکت مایکروسافت که برای دریافت و ارسال ایمیل بکار می رود در مقابل کرمها بسیار آسیب پذیر است. توصیه می شود که از این برنامه استفاده نکنید. برای اطلاعات بیشتر در اینمورد به فصل دوم مراجعه نمایید.

3- برنامه های جاسوس برای گرد آوری اطلاعات شخصی یا Spyware: برنامه جاسوس به برنامه های اطلاق می شوند که بمنظور جمع آوری اطلاعات روی کامپیوتر شما نصب میشود. این برنامه ها می توانند علاوه بر جمع آوری و ارسال اطلاعات باعث نصب برنامه های دیگری، کندی سیستم و بازشدن اتوماتیک پنجره های جدید و متعددی تبلیغاتی شوند. اگر کامپیوتر شما این عوارض را نشان میدهد به احتمال زیاد آلوده شده است.

راههای مقابله با هکرها و آلودگی های امنیتی

جواب: بهترین راه مقابله با هکرها بالا بردن امنیت سیستم های کامپیوتری می باشد. انجام کارهای زیر حداقلی است که باید انجام شوند:

1. نصب آنتی ویروس
2. نصب فایروال (دیواره آتش) یا سد دفاعی
3. نصب برنامه های ضد جاسوسی
4. مدیریت پسوردها
5. استفاده از مرورگرهای امن
6. افزایش امنیت در اینترنت کافه ها
7. پاک کردن ردپای وبگردی
8. رعایت اصول ایمنی

1 - نصب آنتی ویروس

آنتی ویروسها با مشاهده و بررسی محتوای فایل ها به دنبال الگوهای آشنای ویروسها یا کرم های اینترنتی می گردند. در صورت مشاهده این الگوها که به آن Virus Signature گفته می شود، از ورود آن فایل به کامپیوتر تان و یا اجرا شدن جلوگیری می کنند. از شما میپرسند که آیا فایل را حذف کنند و یا سعی در اصلاح آن نمایند.

با توجه به اینکه هر روز هزاران ویروس و کرم و جاسوس جدید تولید میشود، شرکتهای سازنده آنتی ویروس آنها را کشف و جمع آوری می کنند. به این دلیل لازم است برنامه آنتی ویروس تان را زود به زود، مثلا هر روزه، به روز (Update) کنید تا ویروسهای جدید را بشناسد.

یک برنامه خوب و مجانی آنتی ویروس برنامه AVG است که میتوانید از اینجا دریافت کنید. فیلم راهنمای نصب و استفاده از AVG را می توانید از اینجا دریافت کنید.

توصیه میکنیم که سطح ایمنی و ویروس کشی برنامه آنتی ویروس را در حالت High بگذارید تا تمام فایلها ، با هر پسوندی که هستند ویروس کشی شوند و توجه داشته باشید آنتی ویروس AVG حالتی را با عنوان Heuristic دارد ، که به معنی اکتشافی است و در این حالت ویروس کش ، به طرز هوشمندانه ای اقدام به ویرس یابی می کند. توجه داشته باشید خیلی از ویروس هایی که در کامپیوتر شما پنهان شده اند به این روش آشکار می شوند . در حقیقت این نوع ویروس ها دو زیست هستند و مرتبا تغییر می کنند و از این رو ویروس کش ، در حالت عادی نمی تواند آنها را بیابد.

2 - فایروال (دیواره آتش) سد دفاعی

وصل کردن کامپیوتر به اینترنت میتواند هر "آتشی" که در اینترنت هست را به کامپیوتر شما سرایت دهد. بنا براین جود یک دیوار آتش یا سد دفاعی حیاتی است. این دیوار مانع دسترسی برنامه ها و عناصر نامطلوب به کامپیوترتان از طریق اینترنت و یا شبکه های کامپیوتری شوید. بدون دیواره آتش و آنتی ویروس مثل این است که در خانه خود را باز بگذارید و

به مسافرت بروید. دیوار آتش Firewall مانند ایست و بازرسی است که تمامی "چیزهائی" که قصد ورود و یا خروج از کامپیوتر شما دارند را بررسی کرده و اجازه عبور میدهد یا مانع از عبور میشود. با استفاده از دیوار آتش می توانید دسترسی دیگران به کامپیوترتان از طریق اینترنت را محدود کنید. یکی از بهترین فایروالها زون آلارم (Zone Alarm) می باشد. این برنامه بدلیل قابلیتهایی که دارد می تواند کامپیوتر شما را از شر مزاحمین مصون نگاه دارد. این برنامه را می توانید از اینجا دریافت کنید. فیلم راهنمای نصب Zone Alarm را می توانید از اینجا دریافت کنید، همچنین می توانید فیلم راهنمای استفاده از Zone Alarm را از اینجا دریافت کنید.

3 - برنامه های ضد جاسوسی

برای از بین بردن برنامه های جاسوسی حتما از برنامه های ضد جاسوسی حتما استفاده کنید. یکی از بهترین برنامه های ضد جاسوسی برنامه Spybot Search & Destroy است که مجانی می باشد و قابلیت ایمن سازی را علاوه بر یافتن و حذف برنامه های جاسوسی دارد. بیاد داشته باشید که این برنامه ها را هم مانند آنتی ویروس ها باید دائما به روز یا Update کنید. برنامه Spybot را می توانید از اینجا دریافت کنید. فیلم راهنمای نصب و استفاده از این برنامه را هم می توانید از اینجا دریافت کنید.

4- مدیریت پسوردها

کلمات عبور اولین مرحله حفاظت از کامپیوتر و شناسه های شما هستند. کاربران کامپیوتر معمولا در مورد کلمات عبور دو اشتباه بزرگ مرتکب می شوند:

- کلمات عبوری انتخاب می کنند که برای حفظ کردن ساده باشند .
- کلمات عبورشان را نوشته و در جایی که قابل رویت است قرار می دهند

بسیاری از هکرها سعی می کنند با حدس زدن کلمات عبور، وارد سیستم های کامپیوتری شوند. هکرها این کار را با کمک برنامه های شکستن کلمات عبور انجام می دهند. این برنامه ها از لیستی از کلمات مورد استفاده عموم در زبان های گوناگون و همچنین کلمات موجود در دیکشنری، برای یافتن پسوردها استفاده می کنند. برای جلوگیری از هک شدن پسوردتان بهترین کار انتخاب کلمات پیچیده که مخلوطی از اعداد و حروف باشد است.

یک مشکل مرسوم دیگر این است که به دلیل تعدد کلمات مورد نیاز در دنیای جدید، بسیاری از ما از یک کلمه عبور در همه جا استفاده می کنیم. وقتی این کلمه عبور شکسته شود، تمام شناسه ها و اطلاعات ما برای هکرها قابل دسترسی خواهد بود. فرض کنید وقتی دارید از بانک پول می گیرید، کسی به عددی که وارد می کنید نگاه کند و بعد بتواند به کلیه اطلاعات شما دسترسی داشته باشد !

پیشنهاد می کنیم برای مدیریت پسوردهایتان از برنامه Keepass استفاده کنید. این برنامه کلمات عبور شما را در یک بانک اطلاعاتی کاملا رمزگذاری شده ذخیره می کند. این بانک تنها حاوی یک فایل است و در نتیجه می تواند به سادگی از یک کامپیوتر به یک کامپیوتر دیگر منتقل شود. این بانک اطلاعاتی توسط یک کلمه عبور اصلی یا یک key-disk حفاظت شده است. اگر از یک کلمه عبور اصلی استفاده کنید، تنها باید یک کلمه عبور را در یاد نگاه دارید (که حالا می تواند یک کلمه عبور بسیار قوی باشد). بانک اطلاعاتی توسط روش های ریاضی رمزگذاری شده است و هیچ درپشتی یا کلیدی وجود ندارد که بتواند آن را بازیابی کند. برنامه Keepass را می توانید از اینجا دریافت کنید.

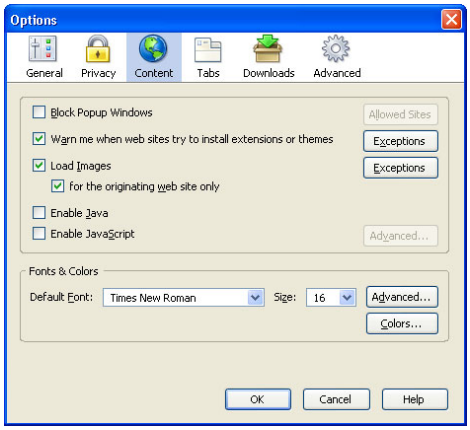
5 - استفاده از مرورگرهای امن

خیلی از برنامه های جاسوسی و Trojanها فقط در صورتی دانلود و در نتیجه فعال می شوند که صفحه مربوطه توسط اینترنت اکسپلورر باز شود ، همچنین خیلی از کرمهای اینترنتی در صورت اجرا شدن و باز بودن اینترنت اکسپلورر گسترش پیدا می کنند . پیشنهاد می کنیم از یک مرورگر دیگر، به جای اینترنت اکسپلورر استفاده کنید و قابلیت Javascript آن را نیز غیر فعال کنید . در این میان مرورگر ها فایرفاکس کارآمد تر و امنتر از سایر مرورگرها می باشد. توصیه میکنیم این مرورگر را نصب کنید. فایرفاکس را می توانید از اینجا دریافت کنید و برای نصب فایرفاکس از فیلم راهنمایی که تهیه کرده ایم استفاده کنید. این فیلم را می توانید از اینجا دریافت کنید.

در ادامه و برای افزایش امنیت فایر فاکس پیشنهاد می کنیم که قابلیت Javascript را در این مرورگر مسدود کنید. اگر پس از انجام اینکار نمی توانید صفحات وبسایتها را بدرستی مشاهده نمایید Javascript را دوباره فعال نمایید. برای غیر فعال کردن Javascript مطابق تصاویر زیر عمل کنید:

1

2



6- **افزایش امنیت در اینترنت کافه ها**: استفاده از کامپیوترهای کافی شاپ ها به این معنا است که شما به احتمال زیاد از کامپیوتری استفاده می کنید که آلوده به برنامه های جاسوسی می باشد. در نتیجه این خطر وجود دارد که نام کاربری، پسورد و وبسایتهایی که بازدید کرده اید ثبت گردیده و بدین ترتیب پلیس بتواند فعالیتهای شما را تحت نظر قرار دهد. متاسفانه استفاده از اینترنت کافه ها در ایران غیر قابل اجتناب است. اما چگونه می توانیم بدون از دست دادن اطلاعات شخصی خود از امکانات اینترنت کافه ها استفاده کنیم؟ توصیه ما این است که برای افزایش امنیت خود در اینترنت کافه ها از راهنمای زیر استفاده کنید:

جلوگیری از به سرقت رفتن اطلاعات شخصی: معمولا در کامپیوترهای کافه اینترنت ها نرم افزارهای جاسوسی بنام کی‌لاگر نصب گردیده است. این نوع نرم افزارها قادر به ضبط اطلاعات تایپ شده در کیبورد می باشند. سپس اطلاعات

شخصی شما مانند آدرس ایمیل و پسورد آن به شخصی که این نرم افزار جاسوسی را نصب کرده است فرستاده خواهد شد و بدین ترتیب ایمیل خود را از دست خواهید داد. برای جلوگیری از سرقت اطلاعات شخصی 3 روش پیشنهاد می شود.

I. **استفاده از پسوردهای ذخیره شده در درایو فلش**: ذخیره پسوردها و نامهای کاربری مورد استفاده در یک فایل موجود در USB Flash Drive (درایو فلش). این نوع درایوها در بازار با قیمتهای مناسب قابل دسترس هستند. بعنوان مثال آدرس ایمیل و پسورد را در فایلی در درایو فلش گذاشته اید و برای ورود به ایمیل از Copy و Paste استفاده میکنید. با انجام اینکار برای ورود به ایمیلتان از کیبورد استفاده نکرده اید، و کیلاگر موفق به ضبط پسورد شما نخواهد شد. البته به یاد داشته باشید که بعضی از کیلاگرها را می توان طوری تنظیم کرد که از صفحه مونیتور عکس بگیرد. اگر در زمان Copy و Paste عکسی گرفته شود ممکن است که پسوردتان را از دست بدهید. برای افزایش اطمینان در این متد می توانید از برنامه های مدیریت پسورد که در درایوهای فلش قادر به نصب شدن هستند استفاده کنید. این نوع برنامه ها پسوردهای شما را به صورت ستاره (*) نشان خواهند داد، در اینصورت حتی اگر عکسی از صفحه در حالت Copy و Paste کردن گرفته شود شما چیزی از دست نخواهید داد. پیشنهاد می کنیم که از نرم افزار Keepass استفاده کنید.

II. **استفاده از کاراکترهای تصادفی**: کیلاگرها اطلاعات تایپ شده را بدین ترتیب ضبط می کنند. در ابتدا آدرس اینترنتی، سپس نام کاربری و در پایان پسورد ثبت می گردد. بعنوان مثال www.hotmail.comsarahj7@hotmail.comsnoopy2 به جاسوس می گوید که وبسایت بازدید شده www.hotmail.com است، آدرس ایمیل sarahj7@hotmail.com است و پسورد برای این ایمیل snoopy2 است. شیوه ای زیرکانه برای فریب کیلاگرها وجود دارد و این استفاده از به اصطلاح نقطه قوت کیلاگرها است که همه چیزهای تایپ شده را ثبت می کنند. برای نمونه به وبسایت hotmail بروید. با استفاده از ماوس در گزینه ID کلیک کنید و حرف اول آی دی خود را تایپ کنید. سپس با استفاده از ماوس به قسمت آدرس بار مرورگر خود بروید و چند حرف بیربط را تایپ کنید. دوباره به فیلد آی دی برگردید و حرف دوم آی دی خود را تایپ کنید، سپس با استفاده از ماوس دوباره به آدرس بار مرورگر بروید و چند حرف بیربط دیگر تایپ کنید. این روش را ادامه بدهید تا زمانی که آی دی و پسورد خود را وارد کرده اید. در اینجا به جای آدرس ایمیل sarahj7@hotmail.com و پسورد snoopy2 این مقادیر بدست می آید: hotmail.comspqmlainsdgsosdgfsodgfdpuouuyhdg2 در اینصورت حتی اگر کیلاگری وجود داشته باشد شخص هکر تنها با تعدادی حروف و اعداد طرف است که نمی تواند از آن هیچ استفاده ای بکند. این روش برای تمامی کیلاگرها موثر است و تاکنون هیچ کدام از کیلاگرها نتوانسته اند که این روش زیرکانه را شناسایی کنند. بیاد داشته باشید که معمولا آسانترین متد، بهترین متد است.

III. **استفاده از کیبوردهای مجازی برای تایپ کردن**: کیلاگرها اطلاعات تایپ شده توسط کیبورد را ثبت می کنند. در این روش ما بجای کیبورد واقعی برای تایپ کردن از یک کیبورد مجازی و بجای انگشتان برای تایپ کردن از ماوس استفاده می کنیم. کیبورد مجازی را می توانید در درایو فلش حمل کنید. برای دریافت کیبورد مجازی اینجا را کلیک کنید. این روش به اندازه روش قبلی قابل اعتماد نیست زیرا برخی از کیلاگرها قابلیت ضبط حروف تایپ شده را در کیبوردهای مجازی دارند. استفاده از این متد در صورت عدم استفاده از روشهای قبلی توصیه می شود.

پاک کردن ردپای وبگردی

اینترنت اکسپلورر، فایرفاکس، اپرا و سایر مرورگرهای اینترنتی با دقت شگفت‌انگیزی می‌توانند فعالیت‌های شما در هنگام آنلاین بودن ثبت کنند و این مسئله فراتر از چیزهایی است که کاربر در بخش History این برنامه‌ها می‌بیند. پاک کردن اطلاعات درون بخش حافظه موقت مرورگر و فایل‌های درون بخشHistory ، نه تنها به شما در افزایش امنیت حریم خصوصی خود کمک می‌کند، بلکه با افزایش فضای مفید هارددیسک، در کارایی کامپیوتر نیز مؤثر خواهد بود.

تا به حال وب سایت‌هایی را دیده‌اید که اگر بار اول وارد آن‌ها شوید، آن‌ها اسم کاربری از شما خواهند پرسید و هر بار که مجدداً وارد آن‌ها شوید، با آن اسم شما را خطاب قرار می‌دهند و مثلاً ورودتان را به آن سایت خوشامد می‌گویند؟ آیا تا به

حال از خود پرسیده‌ایدکه در هنگام استفاده از صندوق پست الکترونیکی خود روی یک کامپیوتر عمومی، باید شناسه کاربری وکلمه عبور خود را وارد کنید، ولی در هنگامی که از خانه می‌خواهید وارد صندوق پست الکترونیک خود شوید، به طور خودکار این اتفاق برایتان می‌افتد؟

پاسخ این سؤال‌ها در کوکی‌ها نهفته است. فایل‌های متنی کم‌حجمی که درون آن‌ها اطلاعات بسیار زیادی در مورد نام پی‌سی، نام کاربری، کلمه عبور، زمان بازدید از وب سایت و ..... ذخیره می‌شوند و سایت مبدا با استفاده از این اطلاعات می‌تواند خدماتی مثل موارد نامبرده را به کاربر ارائه دهد. البته طبق قاعده و در حالت عادی کوکی‌ها را نمی‌توان و نباید تهدیدی برای در معرض خطر قرار دادن امنیت حریم شخصی تلقی کرد. حتی کوکی‌هایی که درون آن‌ها اطلاعات حساسی چون شناسه کاربری و کلمه عبور ذخیره شده است، به طور معمول به خوبی رمزنگاری شده‌اند. با این همه، برخی از کوکی‌ها اغلب همنام سایت مبدا خود هستند و از این طریق می شود نام وبسایت بازدید شده را فهمید. بنابراین مدیریت کوکی ها مهم است.

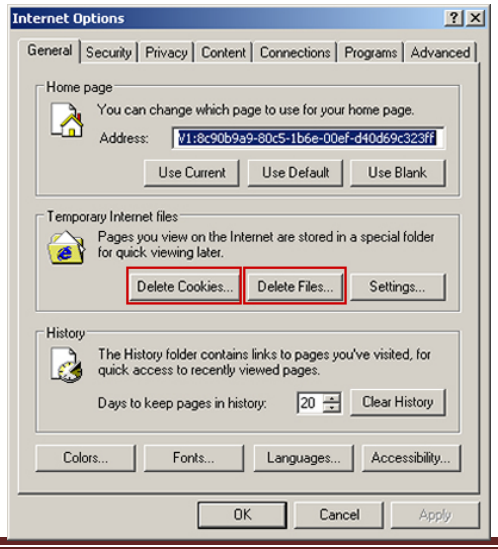
2 شیوه را برای جلوگیری از ثبت و همچنین پاک کردن این نوع اطلاعات به شما پیشنهاد می کنیم:

I. استفاده از برنامه هایی که در USB Flash drive قابل استفاده باشند. با استفاده از برنامه های قابل حمل در این نوع درایوها فایلهای موقت و کوکی ها بجای هارد دیسک کامپیوتر در فلش درایو ذخیره می گردند و بدین ترتیب شما از ذخیره شدن این نوع اطلاعات در کامپیوتر مورد استفاده در اینترنت کافه جلوگیری می کنید. برای دانلود نسخه قابل حمل مرورگر فایرفاکس اینجا را کلیک کنید. همچنین در اینجا می توانید لیست برنامه های قابل حمل را مشاهده نمایید.

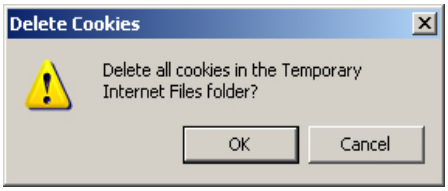
II. اگر به هر دلیلی قادر به استفاده از درایو فلش نیستید برای پاک کردن این اطلاعات در مرورگرهای مختلف مطابق دستورات زیر عمل کنید:

اینترنت اکسپلورر 6:

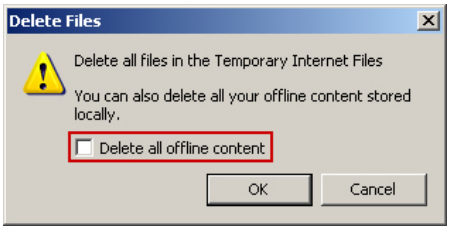
- ✓ در Internet Explorer روی Tools کلیک کنید.
- ✓ گزینه Internet Options را انتخاب کنید.



- ✓ گزینه General را انتخاب کنید.
- ✓ قسمت Temporary Internet Files را نگاه کنید.



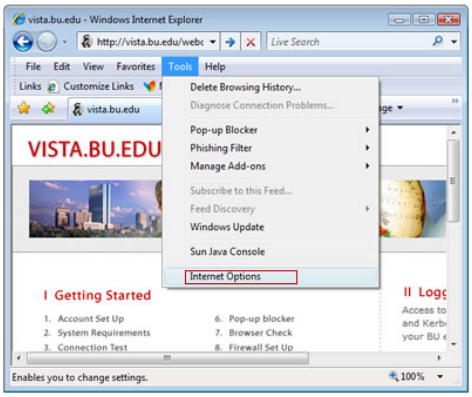
- ✓ روی دکمه Delete Files کلیک کنید و روی Ok کلیک کنید.

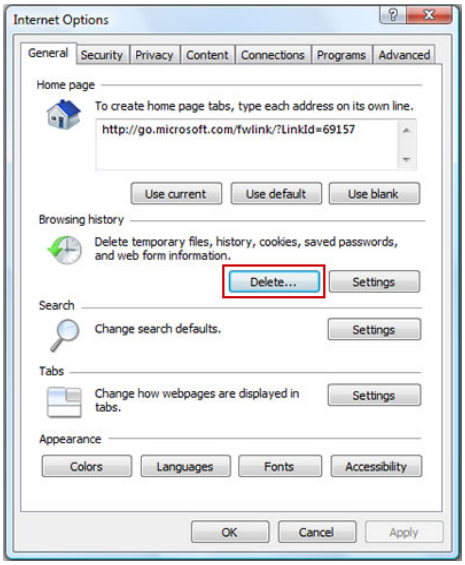


- ✓ روی دکمه Delete Cookies کلیک کرده و Ok که ظاهر میشود را بزنید.
- ✓ روی دکمه Clear History کلیک کنید و روی Yes بزنید.
- ✓ در نهایت روی دکمه Apply کلیک کنید و با زدن کلید Ok از Internet Options خارج شوید.

I. اینترنت اکسپلورر 7:

- ✓ در Internet Explorer روی Tools کلیک کنید
- ✓ گزینه Internet Options را انتخاب کنید.





- ✓ قسمت Browsing history را نگاه کنید.

- ✓ در صفحه باز شده روی دکمه Delete all کلیک کنید و روی Yes بزنید.

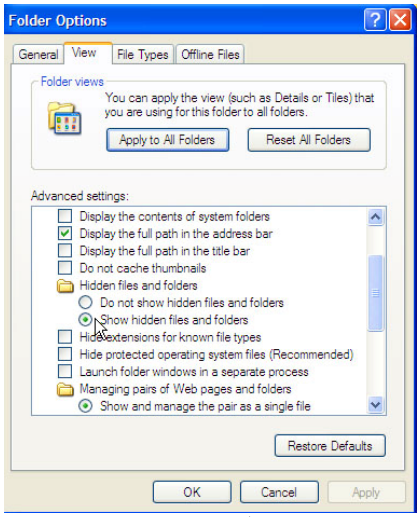
II. فایر فاکس:

- ✓ در فایرفاکس روی Tools کلیک کنید
- ✓ گزینه Clear Private Data را انتخاب کنید.

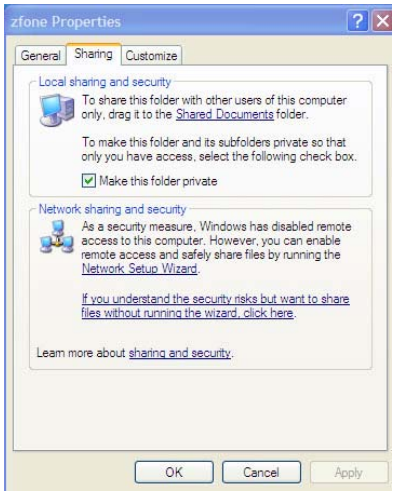
- ✓ گزینه های زیر را که با فلش مشخص شده اند تیک بزنید و سپس روی دکمه Clear Private Data Now کلیک کنید.

رعایت سایر اصول ایمنی برای سیستم عامل ویندوز

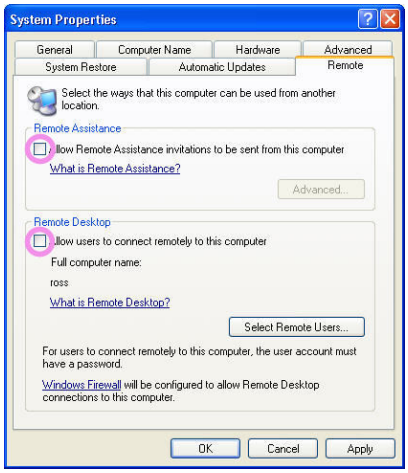
I. نشان دادن پسوند فایلها: سیستم عامل ویندوز پسوند فایلها را مخفی نگاه می دارد. بعنوان مثال اگر شما مایکروسافت آفیس نامه ای را تایپ کرده اید و نام فایل را "letter" گذاشته اید این فایل را با نام "letter" در پوشه ای که قرار دارد خواهید دید. حال اگر شخص هکر یا پلیس پس از دسترسی به کامپیوتر شما برنامه ای جاسوسی در آن قرار داده باشد و بخواهد که شما از اجرا و نصب آن آگاهی نداشته باشید از عدم نشان دادن پسوند فایلها استفاده خواهد کرد. فقط کافی است که فایل letter.doc را حذف کرده و ویروس مورد نظر را با این اسم letter.doc.exe در کامپیوتر شما قرار دهد. این فایل سپس به صورت letter.doc نشان داده خواهد شد و بدین ترتیب شما فکر خواهید کرد که این فایل مورد نظر شماست. زمانی که قصد اجرای این فایل را داشته باشید ویروس مورد نظر بدون اطلاع شما نصب خواهد شد. برای جلوگیری از نصب برنامه های جاسوسی با استفاده از این روش پیشنهاد می کنیم که ویندوز را طوری تنظیم کنید تا پسوند فایلها را نشان دهد. برای انجام اینکاریکی از فولدرهای خود را باز کنید. سپس از منوی بالایی روی "Tools" کلیک کنید و گزینه "Folder Options" را انتخاب کنید. سپس روی "View" کلیک کنید. در اینجا به قسمت "Hidden files and folders" بروید و گزینه "Show hidden files and folders" را انتخاب کرده و سپس روی OK کلیک کنید.



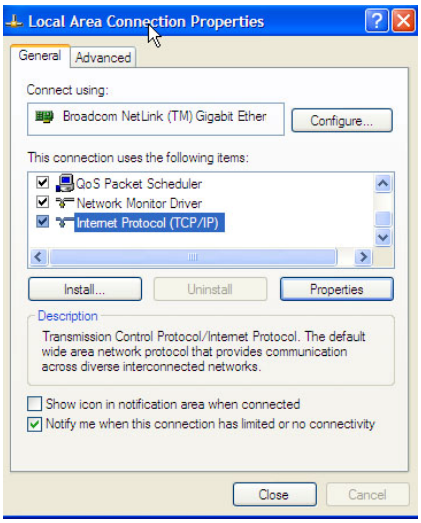
II. محدود کردن دسترسی: اجازه شریک نشدن فایل ها از مهمترین عوامل بالابردن امنیت است. اگر چند نفر از کامپیوتر شما با نامهای کاربری متفاوت استفاده می کنند لازم است که فولدرهای خود را از معرض دید کاربران دیگر دور نگاه دارید. در اینصورت اگر نام و پسورد یوزرهای دیگر هک بشود فولدرهای شما که حاوی فایلهای متعلق به شما می باشد قابل دسترسی برای هکر نخواهد بود. برای انجام اینکار روی فولدر مورد نظر راست کلیک کنید وگزینه Properties را انتخاب کنید. سپس روی گزینه "Sharing" کلیک کنید و "Make this folder private" را تیک بزنید. و سپس روی دکمه OK کلیک کنید. تصویر مقابل را با بدین منظور مشاهده کنید. ویدیوی آموزشی اینکار را می توانید از اینجا دریافت کنید.



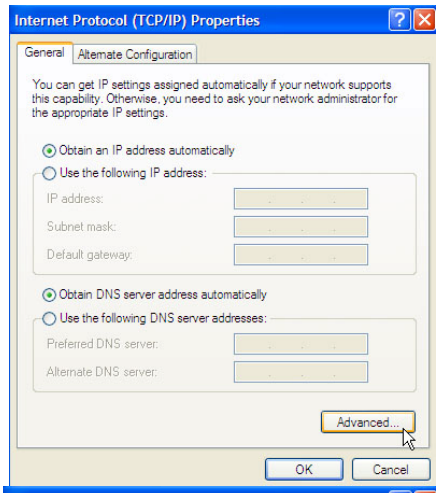
III. غیر فعال کردن دسترسی از راه دور: برای جلوگیری از دسترسی دیگران به کامپیوتر شما از راه دور لازم است که سرویس Remote Assistance را غیر فعال کنید. برای انجام اینکار روی منوی Start کلیک کنید و سپس روی My Computer راست کلیک کنید و سپس گزینه Properties را انتخاب کنید. در اینجا روی گزینه Remote کلیک کنید و این گزینه های Remote Assistance و Remote Desktop را غیر فعال کنید. تصویر مقابل را با بدین منظور مشاهده کنید.



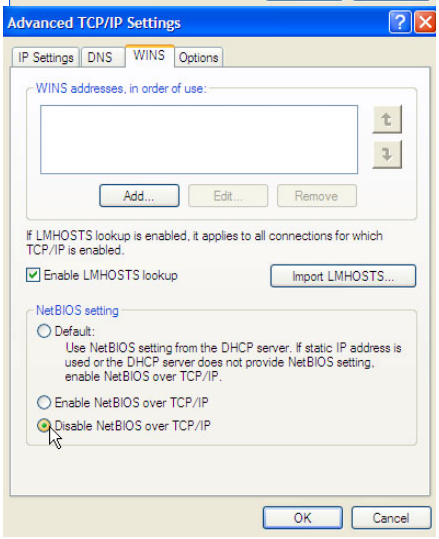
IV. **غیر فعال کردن** NetBIOS: ممکن است فایلهای شما در کل اینترنت به اشتراك گذاشته شوند. همچنین نام کاربری و کامپیوتر شما براي دیگران قابل از طریق اینترنت قابل مشاهده باشد. برای جلوگیری از به اشتراک گذاشتن فایلهای شخصی شما در اینترنت لازم است که NetBIOS را غیر فعال کنید. در ابتدا ویندوز اکسپلورر را باز کنید و روی My Network places راست کلیك کنید. سپس Properties را انتخاب کنید و روی Local Area Networkراست کلیك کنید. Properties را انتخاب کنید و Internet protocol TCP/IP را انتخاب کنید.



در ادامه روی Properties کلیك کنید و گزینه Advanced را انتخاب کنید.



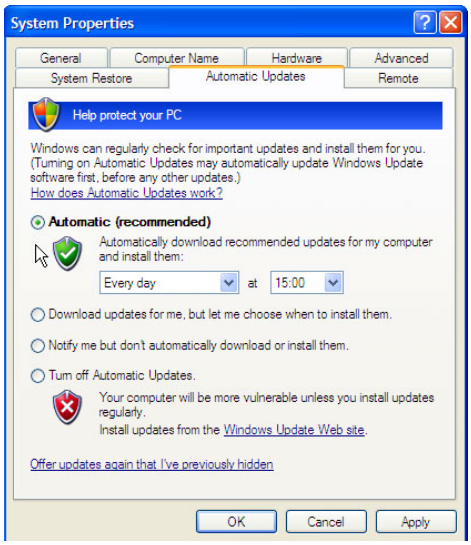
سپس وارد قسمت WINS شوید و Disable NetBIOS over TCP/IPرا انتخاب کنید و OK را کلیك کنید



برای ثبت تغییرات باید کامپیوتر خود را Restart کنید.

V. از کار انداختن System Restore: همانطور که می دانید فایلهایی که پسوند های سیستمی مثل dll، exe و غیره داشته باشند ، پس از پاک کردن یا اعمال تغییرات در System Restore ذخیره می شوند و این مسئله زمانی خطر ساز می شود که یک فایل ویروسی را به صورت دستی یا به کمک برنامه های ضد ویروس یا ضد Spyware حذف کرده اید. در واقع ویندوز این فایلها را در جایی دیگر حفظ کرده است و همچنان ویروس به فعالیت خود ادامه می دهد. برای از کار انداختن System Restore این مراحل را انجام دهید. در ابتدا به Control Panel بروید و روی System کلیک کنید. سپس روی System Restore کلیک کنید و گزینه Turn off System Restore on All Drive را انتخاب کنید.

IV. گرفتن منظم وصله های امنیتی Patches: با گذر زمان اشکالات جدید در نرم افزارهای مختلف شناسایی می شوند که امکان سوءاستفاده را برای هکرها بوجود می آورند. پس از شناسایی هر اشکالی شرکت تولید کننده محصول اقدام به نوشتن وصله های مناسب برای افزایش امنیت و از بین بردن راه های نفوذ به سیستم می کنند. این وصله ها بر روی سایت های وب شرکت ها عرضه می شود و کاربران باید برای تامین امنیت سیستم خود همواره آخرین نسخه های وصله ها را گرفته و بر روی سیستم خود نصب کنند. می توانید ویندوز خود را طوری تنظیم کنید که بطور اتوماتیک جدیدترین وصله های امنیتی را نصب کند. برای انجام اینکار روی منوی Start کلیک کنید و سپس روی My Computerراست کلیک کنید و سپس گزینه Properties را انتخاب کنید. در اینجا روی گزینه Automatic Updates کلیک کنید و گزینه Automatic (recommended) را فعال کنید. تصویر زیر را با بدین منظور مشاهده کنید:



V. از باز کردن فایلهایی با پسوندهای **exe/com/bat** جدا خودداری کنید.

VI. قطع اتصال به اینترنت در مواقع عدم استفاده: به خاطر داشته باشید که بزرگ راه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند. قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد. این موارد در نزد کاربران خانگی و افرادی که تلفنی به کامپیوتر متصل می شوند به دلیل محاسبه هزینه اتصال کمتر اتفاق می افتد اما در ادارات و ارگانها و مکانی هایی که دایم می توانند به اینترنت متصل باشند دیده می شوند بدون هیچ کارایی به اینترنت متصل می مانند.

VII. هرگز اسم کامپیوتر (Computer Name) خود را واقعی ندهید . هکرها می توانند اسم کامپیوتر شما و در نتیجه اسم شما را بیابند و برای جلوگیری از این کار یک اسم مستعار برای خود انتخاب کنید . همچنین از وارد کردن اسم و مشخصات واقعی خود در برنامه هایی مثل Photoshop و غیره که در زمان نصب از شما اسم و مشخصات می خواهند نیز خودداری کنید

فصل دوم: پیگیری پلیسی - Forensic

در صورتی که پلیس به کامپیوتر شما دسترسی پیدا کند یا شبکه اینترنت شما تحت نظر باشد، آنها سعی خواهند کرد تا ردپاهایی که شما بر جا گذاشته اید را بیابند و مدارک یافت شده را بر علیه شما استفاده کنند. این ردپاها بر روی هارد دیسک کامپیوتر ثبت می گردد. سیستم عامل ویندوز تمام فعالیتهای صورت گرفته در کامپیوتر (مانند فایلهای اجرا شده، وبسایتهای بازدید شده، ایمیلهای فرستاده شده و پسوردهای مورد استفاده و ..) را به گونه ای که قابل مشاهده نباشند در تاریخچه خود ذخیره می کند. پس از پایان کار خود با کامپیوتر اگر کوکی ها، تاریخچه مرورگر و .. را پاک نکنید اطلاعات مربوط به فعالیت شما در کامپیوتر باقی مانده و پلیس به آسانی می تواند به آنها دسترسی پیدا کند. پلیس قادر به جمع آوری مدارک زیر و استفاده از آن بر علیه شما خواهد بود:

1. آی پی کامپیوتر شما، مثلا با استفاده از سایتهای ایرانی مانند بلاگفا و پرشین بلاگ
2. فایلهای ذخیره شده در هارد دیسک
3. ایمیلهای دریافتی و فرستاده شده
4. متن یا صدای مکالمات شما با استفاده از مسنجرها (یاهو مسنجر و گوگل تاک)

برای جلوگیری از برجای گذاشتن هر گونه ردپا و در نتیجه استفاده از آن بر علیه خودتان راهکارهای زیر را به شما پیشنهاد می کنیم.

1. جلوگیری از ردگیری شما با استفاده از آی پی
2. افزایش امنیت هارد دیسک
3. افزایش امنیت فایلها و فولدرها
4. پاک کردن هیستوری مرورگرها
5. افزایش امنیت ایمیل با استفاده از رمزنگاری
6. افزایش امنیت چت کلاینتها و استفاده از کلاینتهایی که امنیت بالاتری دارند
7. از بین بردن سریع هارد درایو در صورت احتمال دستگیری

ردگیری شما از طریق آی پی

به هر کامپیوتری که به اینترنت متصل شود شماره ای اختصاص می یابد و بوسیله آن کامپیوتر شما در اینترنت با آدرسی منحصر به فرد شناخته می شود که تا حدی مشابه آدرس پستی است. این آدرس در واقع آدرس آن کامپیوتر خاص در شبکه است و از طریق آن دیگر کامپیوتر ها می توانند با کامپیوتر مذکور ارتباط برقرار نمایند و یا به منابع آن دسترسی پیدا کنند . این شماره آی پی نام دارد و بصورت زیر نوشته می شود:

xxx.xxx.xxx.xxx که منظور از xxx عددی بین 0 تا 255 است. مثلا ممکن است آدرس شما به صورت 195.219.176.69 باشد. حتي اسمهايي مثل http://www.yahoo.com/ که براي اتصال استفاده ميكنيد، در نهايت بايد به یک آی پی تبدیل شود، تا شما سایت یاهو را ببینید.

امنیت استفاده از شرکتهای خدماتی وبلاگ مانند بلاگفا

بسیاری از کاربران اینترنتی در ایران برای درج خاطرات روزانه یا بیان عقاید سیاسی و اجتماعی خویش که بعضا در تضاد با جمهوری اسلامی قرار دارد از امکانات وبلاگ استفاده می کنند. همانطور که گفتیم وبسایتها توانایی ثبت آی پی شما را دارند و پلیس با استفاده از این آی پی می تواند شما را بیابد و دستگیر کند.

2 نوع وبسایتهای خدمات وبلاگ وجود دارند. وبسایتهای خارجی مانند بلاگر و وردپرس و وبسایتهای ایرانی مانند پرشین بلاگ و بلاگفا. سایتهای ایرانی پرشین بلاگ و بلاگفا بر اساس قوانین رژیم اسلامی فعالیت می کنند. این بدین معنا است

که آی پی های ثبت شده توسط وبسایتهای ایرانی می تواند براحتی در دسترس وزارت اطلاعات قرار گیرد، به این دلیل ساده که این وبسایتها اعلام کرده اند که در محدوده قوانین جمهوری اسلامی فعالیت می کنند و سرورهای آنها در ایران قرار دارند.

اگر شما یک فعال اجتماعی هستید و یا اینکه در خاطرات خویش مسایلی را درج می کنید که فکر می کنید برایتان دردسر ساز می شوند **اکیدا از استفاده از بلاگفا، پرشین بلاگ و سایر وبسایتهای ایرانی که خدمات بلاگ ارائه می کنند خودداری کنید. استفاده از وبسایتهای ایرانی بمانند دعوت از پلیس برای دستگیری شماست!**

پیشنهاد می کنیم از خدمات بلاگر یا وردپرس استفاده کنید.

با IP هرگز در اینترنت پنهان نخواهیم بود

یک IP یک الزام فنی محسوب می شود و هرگز با این سیاست در شبکه تدوین و تعریف نشده است که کاربر را افشا کند ؛ اما تنها برای شناسایی کاربر یک عدد منحصر به فرد اجباری بوده است. اما این امر ممکن است مشکل ساز شود ؛ یک هکر مبتدی با دانستن IP فعلی شما در زمان اتصال شما به اینترنت می تواند وارد سیستم کامپیوتر شما شده و تمام کامپیوتر شما را در دست بگیرید.

آی پی شما اهمیت بسیار زیادی دارد. پلیس می تواند از طریق آی پی شماره تلفن و مکان جغرافیایی شما را بیابد. در واقع و به زبانی ساده تر پلیس با داشتن آی پی می تواند به منزل شما مراجعه کند. اگر علاقمند هستید آدرس آی پی خود را بدانید و اینکه آی پی شما می تواند چه اطلاعاتی فراهم کند به این صفحه مراجعه کنید. بیاد داشته باشید که پلیس در ایران به سیستم مخابرات دسترسی دارد و از طریق آی پی شماره تلفن و آدرس خانه شما را خواهند یافت. برای جلوگیری از ثبت آی پی لازم است که شیوه های معمول بدست آوردن آی پی را برای شما توضیح بدهیم:

- **از طریق بازدید وبسایتها**: اکثر وبسایتها دارای امکاناتی هستند که خصوصیات یک کاربر همراه با آی پی وی را ثبت می کنند.

- **از طریق ایمیل**: هنگامي که شما ایمیلی را دریافت می کنید، معمولاً آدرس آی پی شخص فرستنده در آن ایمیل وجود دارد. ابتدا باید با رفتن به قسمت تنظیمات ایمیل خود آن را در حالتي قرار دهید که تمامي Header نامه را به شما نشان دهد که با کمي گردش در قسمت تنظیمات ایمیل خود آن را پیدا خواهید کرد. حال به بالاي ایمیل دقت کنید و به دنبال عبارت Received: from باشید. شما معمولاً دو یا چند بار عبارت "Received: from" را در بالاي ایمیل خواهید دید که معمولاً بعد از Message ID قرار مي گیرد. آدرس آی پی فرستنده ایمیل درست در ابتدای این عبارت قرار می گیرد. از سوي دیگر بسیاری از میزبانان ایمیل، راه آسانتری هم برای کمک به شما در نظر می گیرند به این صورت که قسمتی با نامی شبیه به X-Originating-Ip برای شما قرار مي دهند و آی پی فرستنده نامه را در آنجا قرار دارد.
- **از طریق مسنجرها**: هنگامي که با کسی روی مسنجر صحبت مي کنید باید کامپیوترهای شما به هم متصل باشند اما Yahoo یا MSN مسنجر میزبان خود را بین شما و فرد مقابل قرار مي دهند به این صورت که شما و دوستتان هر دو به سرور مسنجر متصل می شوید و همه پیامها از آن عبور می کنند. این بدین معنا است که پیام شما در ابتدا وارد سرور مسنجر مي شود و سپس از طریق سرور مسنجر به فرد مقابلتان می رسد و بالعکس. در اینمورد استثنائاتی وجود دارد، بطور مثال زمانی که شما و دوستتان در یک بازی مسنجری شرکت کنید یا فایلی را برای همدیگر ارسال کنید دو کامپیوتر به طور مستقیم به هم متصل می شوند. در اینصورت آی پی شما را می شود از طریق مسنجر بدست آورد.
- **از طریق مهندسی اجتماعی** (Social Engineering): به منظور تدارک و یا برنامه ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص (روابط عمومی مناسب و ...)، سعی می نماید به اطلاعات حساس کامپیوتر شما دستیابی و یا به آنان آسیب رساند .

هکرها با بهره گیری از ایجاد حس اعتماد سعي ميكنند شيوه هاي مختلف مهندسي اجتماعی را از طريق ياد گرفتن ديدگاه هاي روانشناسي پياده سازند، آنچه كه براي آنها اهميت دارد اين است كه بتوانند احساسات و حالتهاي ساختگي را به محيط اطرافشان كاملا القا نمايند. مهمترين شيوه هايي كه نفوذگران به كار ميگيرند تا اعتماد ديگران را جالب نمايند عبارتند از: جعل هويت، خود را مورد توجه ديگران قرار دادن، هم عقيده نشان دادن خود با ديگران، جعل مسئوليت ديگران يا دادن اطلاعات و در آخر بهره برداري از دوستي هاي ديرينه. صرفنظر از شيوه هاي گفته شده، هدف اصلي اين ميباشد كه افراد قانع شوند تا فردي كه بر مهندسي اجتماعی تكيه كرده است فردي قابل اعتماد است و ميتوان به وي اطلاعات بسيار حساس خود را داد. جعل هويت به معناي اين است كه يک شخصيت بسازيد و سپس نقش آن را بازي كند به عنوان مثال: سلام من رضا هستم و از اداره مخابرات تماس میگیریم در اینجا مشکلی پیش اومده و ما احتیاج به پسورد شما داریم.

نحوه پیشگیری از حملات مهندسی اجتماعی

1. به تلفن ها ، نامه های الکترونیکی و ملاقات هائی که عموما ناخواسته بوده و در آنان از شما درخواست اطلاعاتی خاص در مورد اطلاعات شخصی می گردد ، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید . در صورتی که یک فرد ناشناس ادعا می نماید که از یک سازمان معتبر است ، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب تکلیف کنید .
2. هرگز اطلاعات شخصی خود را (مثلا" ساختار و یا شبکه ها) در اختیار دیگران قرار ندهید ، مگر این که اطمینان حاصل گردد که فرد متقاضی مجور لازم به منظور دستیابی به اطلاعات درخواستی را دارا می باشد.
3. هرگز اطلاعات شخصی خود را در یک email افشاء نکرده و به نامه های الکترونیکی ناخواسته ای که درخواست این نوع اطلاعات را از شما می نمایند ، پاسخ ندهید (به لینک های موجود در اینگونه نامه های الکترونیکی ناخواسته نیز توجهی نداشته باشید) .
4. هرگز اطلاعات حساس و مهم شخصی خود را بر روی اینترنت ارسال ننمائید . قبل از ارسال اینگونه اطلاعات حساس ، می بایست Privacy وب سایت مورد نظر به دقت مطالعه شده تا مشخص گردد که اهداف آنان از جمع آوری اطلاعات شخصی شما چیست و نحوه برخورد آنان با اطلاعات به چه صورت است.

برای کاربران داخل ایران پیشنهاد می کنیم که قبل از استفاده از اینترنت حتما آی پی خود را با استفاده از شیوه ای مناسب پنهان کنید. پیشنهاد می کنیم که از روش زیر استفاده کنید.

استفاده از Tor

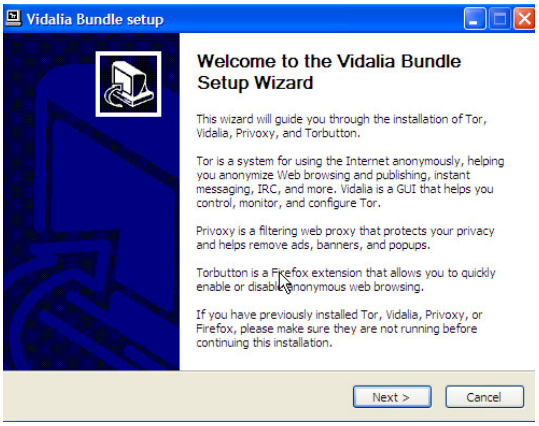
Tor اسم نرم افزاری مجانی است که آن را می توان به شبکه ای از تونلهای مجازی تشبیه کرد. این شبکه شامل چند سرور بزرگ و تعداد بسیار زیادی از کامپیوترها در سرتاسر جهان است. مدل کار Tor کاملا ساده است: شما به این شبکه وصل میشوید... سپس Tor تمام سرورها را به ترتیب پهنای باند لیست میکند... و سه تا از بهترین پهنای باندها را برای شما انتخاب کرده و آن ها را به هم وصل میکند... سپس شما را به سرور اولی وصل میکند... و چون سرور اول به دومی و دومی به سومی وصل است شما اینترنت را از دریچه سرور سوم میبینید و هم IP شما عوض میشود و هم از محدودیت ها میگذرید.

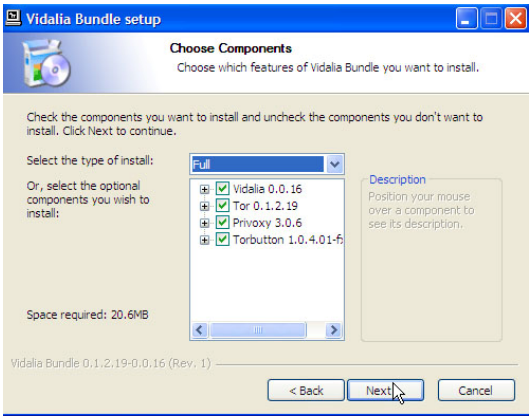
یک مثال Tor: یک سرور در آلمان را به یک سرور در ایرلند وصل میکند و سپس سرور ایرلند را به سروری در ایالت اوهایو در آمریکا وصل میکند... حالا شما رو به سرور اولی که در آلمان بود وصل میکند و از طریق آن سرور شما با گذشت از سرور ایرلندی به سرور آمریکایی وصل میشوید... اگر IP شما در ایران 80.192.192.192 است بعد از این عملیات به 88.168.250.3 تبدیل می شود. به این ترتیب شما در اینترنت پنهان خواهید.

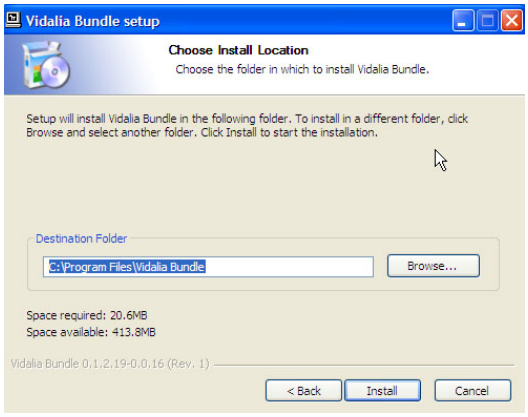
برای نصب Tor مراحل زیر را انجام دهید:

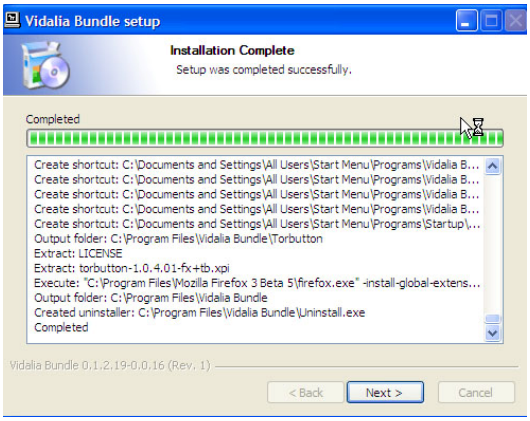
I. در ابتدا لازم است که مرورگر فایرفاکس را نصب کنید. ویدیوی آموزشی نصب و استفاده از فایر فاکس را می توانید از اینجا دریافت کنید.

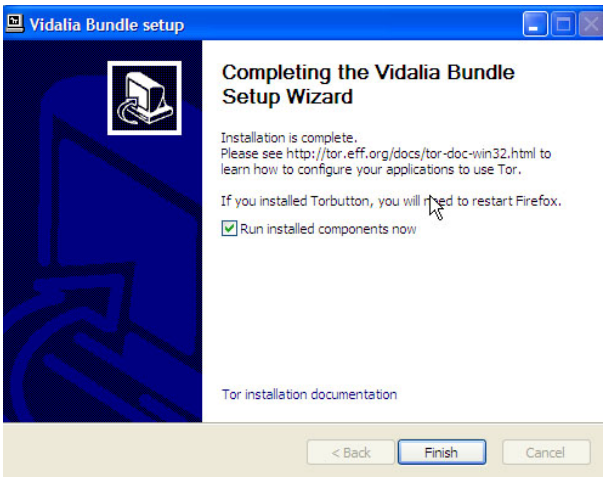
II. Tor را می توانید از اینجا دریافت کنید. Tor در مجموعه برنامه ای به نام Vidalia Bundle وجود دارد. برای نصب این مجموعه از تصاویر زیر استفاده کنید.

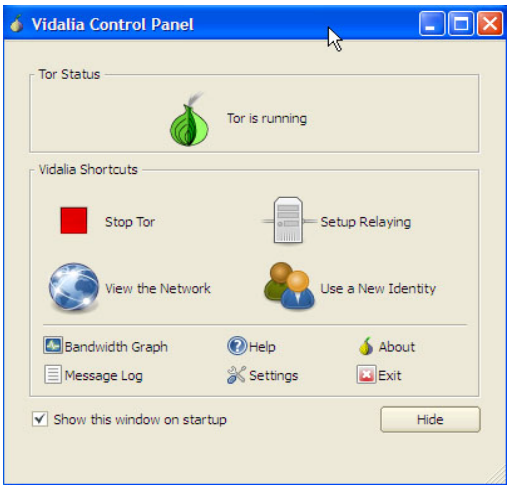


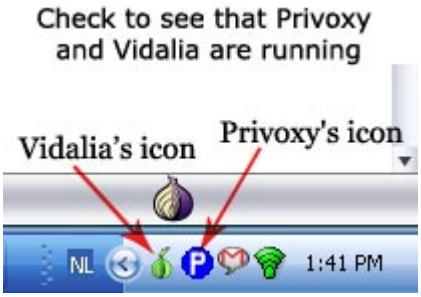




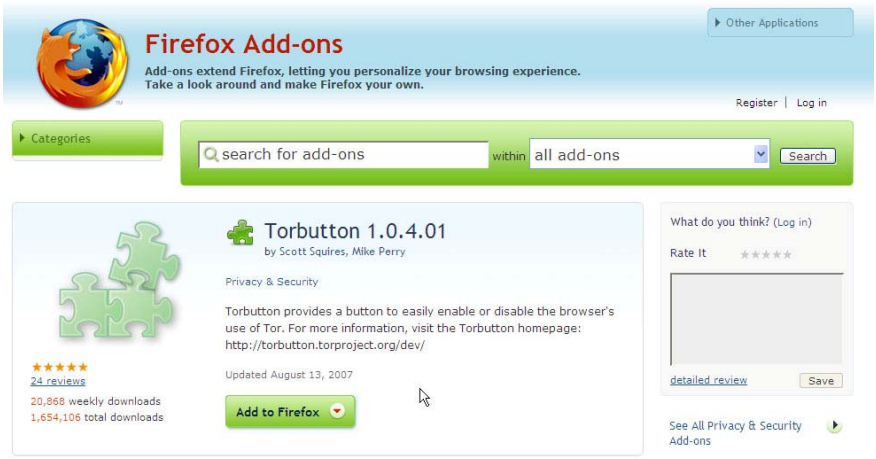


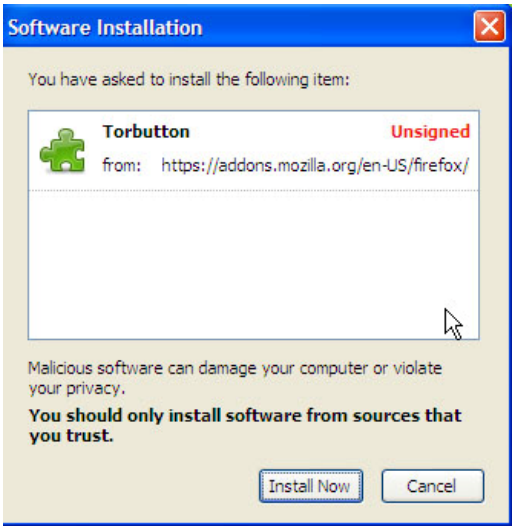




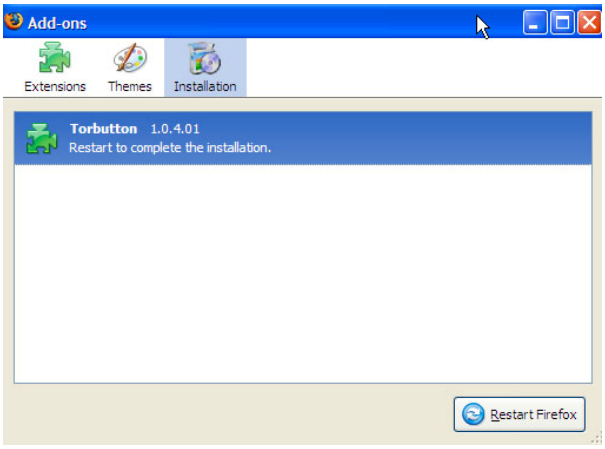


تنظیمات بعد از نصب: لازم است که پلاگین Torbutton را برای فایرفاکس دانلود و نصب کنید. این پلاگین را می توانید از اینجا دریافت کنید.

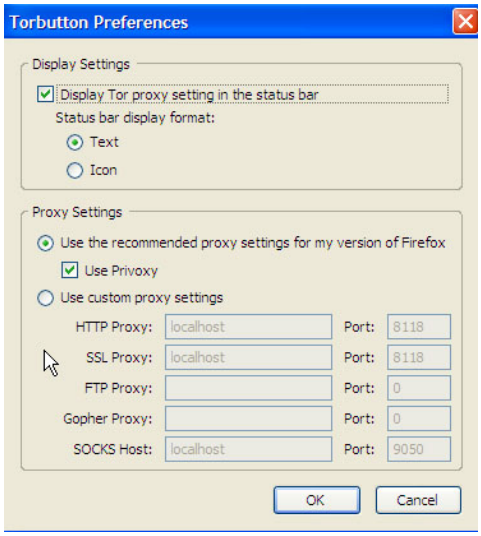




در ادامه برای نصب Torbutton روی Install Now کلیک کنید.



پس از نصب لازم است برای ثبت تغییرات فایرفاکس را ریستارت کنید.



پس از نصب این پلاگین به منوی Tools در فایرفاکس بروید و گزینه Add-ons را انتخاب کنید. سپس روی گزینه Options در Torbutton کلیک کنید و در قسمت Proxy Settings گزینه Use Privoxy را تیک بزنید.

پس از نصب و اجرای تنظیمات حالا زمان استفاده از این نرم افزار است. فایرفاکس را باز کنید و سپس تصویر مقابل را نگاه کنید:

همانطور که مشاهده می کنید این تصویر گوشه پایین مونیتور، جایی که ساعت در آن قرار دارد است. Tor Disabled بمعنای این است شما از Tor استفاده نمی کنید. برای استفاده از پراکسی کافی است یکبار روی این نوشته کلیک کنید. سپس این نوشته به Tor Enabled تبدیل شده و رنگ آن از قرمز به سبز تبدیل می شود. این بمعنای این است که شما از پراکسی استفاده می کنید.

افزایش امنیت هارد دیسک

پلیس قادر به این خواهد بود که فایلهایی را که شما مدتها پیش از روی کامپیوتر خود حذف کرده اید دوباره بازیابی کند. در واقع وقتی که فایلی از روی هارد درایو پاک میشود در اصل رابطه بین آن فایل و ویندوز قطع میشود و خود دیتا و اطلاعات فایل مورد نظر بر روی هارد باقی می ماند و هر وقت که نیاز باشد بر روی فضایی که فایل قدیمی پاک شده قرار داشت اطلاعات جدید باز نویسی میشوند و بعد از این مسئله دیگر دسترسی به فایل قدیمی کمی سخت میشود. با نرم افزارهای بازیابی که امروزه کم و بیش برای همه قابل دسترسی است بازگرداندن فایلهای پاک شده بسیار ساده و راحت شده حتی بعد از فرمت و پارتیشن بندی هم باز میشود به فایلهای قدیمی دسترسی پیدا کرد. این مسئله همانقدر می تواند بسیار دردسر ساز باشد زیرا فایلهایی را که شما فکر می کنید پاک شده اند را با چند کلیک دوباره بازیافت. برای افزایش امنیت هارد دیسک و فایلها و پوشه های موجود در آن نکات زیر را رعایت کنید:

رمز نگاری هارد دیسک، فایلها و پوشه ها بهترین راه برای جلوگیری از دستیابی پلیس به اطلاعات ثبت شده شما روی هارد دیسک می باشد. نرم افزارهای متعددی در این ضمینه وجود دارند. پیشنهاد ما این است که برنامه رایگان و عالی TrueCrypt را که برای برای کدگذاری (Encrypt) کردن اطلاعات کامپیوتر مناسب است را استفاده کنید. این برنامه توانایی استفاده از 11 الگوریتم کدگذاری مختلف را دارد و می تواند کل درایو یا مثلاً کل دیسک شما را کدگذاری کند تا اطلاعات آن از دسترسی دیگران در امان بماند. تا لحظه رمزگشایی، درایو TrueCryptچیزی بیشتر از مجموعه ای از اعداد اتفاقی به نظر نمی رسد چرا که کل فایل سیستم رمزگذاری شده است (یعنی اسم فایل ها، اسم پوشه ها، محتویات فایل ها و حتی فضای خالی. شما می توانید درایو های مجازی محافظت شده بسازید و اطلاعات محرمانه خود را در آن نگهداری کنید. از ویژگی های خوب این برنامه می توان به داشتن نسخه قابل حمل (Portable) ، و سرعت خوب آن اشاره نمود. این برنامه را می توانید از اینجا دریافت کنید.

افزایش امنیت فایلها و فولدرها

برای افزایش امنیت فایلها و فولدرها نکات زیر را رعایت کنید:

I. رمزگزاری: بسیاری از کاربران امروزه با استفاده از نرم افزارهای مختلف اقدام به برقراری امنیت برای فایل های خود می کنند. به عنوان مثال کاربری قصد دارد تا مانع از دسترسی دیگران به فایل ها و اطلاعات شخصی خود شود ، برای این کار می توان از نرم افزارهای حفاظتی استفاده نمود و با ایجاد محدودیت های دسترسی به راحتی این عمل را انجام داد. همچنین ممکن است کاربری قصد داشته باشد از اطلاعات حفاظت شده خود تنها خود و کاربر دیگری استفاده نمایند، در چنین شرایطی با قرار دادن رمز عبور بر روی اطلاعات مورد نظر و در اختیار قرار دادن این رمز به کاربر مورد نظر دیگر این مشکل نیز به راحتی حل می شود. در اینجا نرم افزاری را به شما معرفی می کنیم که به وسیله آن قادر خواهید بود تا از فایل ها و پوشه های خود حفاظت کنید.

My Lockbox نام نرم افزاری می باشد که به وسیله آن کاربران قادر می باشند به راحتی و تنها با چند کلیک فایل ها و پوشه های مورد نظر خود را تحت حفاظت این نرم افزار قرار داده و مانع از دسترسی دیگران به آن ها شوید. همچنین به کمک این نرم افزار می توان یک پوشه را به همراه محتویات آن ها به طور کامل از دید دیگر کاربران مخفی نمود. قابلیت قرار دادن رمز عبور برای یک فایل ، پوشه و یا یک درایو از هارد نیز از دیگر ویژگی های این نرم افزار می باشد.

III. حذف دایمی: شاید برایتان غیرمنتظره باشد ولی باید بدانید که وقتی فایلی را پاک می کنید، در اصل هیچ چیز پاک نمی شود. کامپیوتر شما فقط آن قسمت از حافظه را که قبلا توسط آن فایل اشغال شده بود، با عنوان «بدون استفاده «علامت می زند. بازیابی اطلاعات از این مکان ها ساده است و برنامه های زیادی نیز به این منظور نوشته شده اند. جاهای بسیار دیگری هم روی کامپیوتر هستند که برنامه ها رد خود و اطلاعات شخصی شما را باقی می گذارند. برای مثال، وب سایت هایی که جدیدا به آن ها سر زده اید یا بخش هایی از اسنادی که تازه روی آن ها کار می کرده اید. به همین دلیل است که دانستن این نکته و اطلاع داشتن از شیوه اصلاح آن بسیار مهم است .برای حذف فایلها بدون قابلیت بازیابی باید از برنامه هایی استفاده کنید که فایلها را کلا و کاملا از روی کامپیوتر شما برای همیشه حذف خواهند کرد. File Shredder نام نرم افزاری می باشد که با استفاده از آن دیگر پلیس قادر به یافتن فایلهای حذف شده نخواهد بود. این برنامه را می توانید از اینجا دریافت کنید.

پاک کردن هیستوری مرورگرها

همانطور که گفتیم تاریخچه یا همان هیستوری مرورگر شما گشت گذارهایتان در اینترنت را ضبط و برای استفاده های بعدی خصوصا در هنگامی که آفلاین هستید نگه داری می کند، بنابراین هیستوری یکی از بهترین و ساده ترین چیز هایی است که سایر افراد می توانند با استفاده از آن سر از رمز و راز کار شما در بیاورند. از طرفی ممکن است اصلا برای شما خوشایند نباشد تا بعد از هر وبگردی کلیه اطلاعات هیستوری را پاکسازی و خدف نمائید. برای پاک کردن ردپاهای بر جا مانده می توان از نرم افزارهایی استفاده کرد که این کار را انجام می دهند. نرم افزار پیشنهای ما Internet Sweeper است که بطور مجانی در اختیار کاربران اینترنتی قرار دارد. این نرم افزار را می توانید از اینجا دریافت کنید.

افزایش امنیت ایمیل

برای افزایش امنیت در ارسال و دریافت ایمیل پیشنهاد می کنیم 3 نکته زیر را رعایت کنید.

I. استفاده از رمزنگاری
II. استفاده از ایمیل کلاینتهایی که امنیت بالایی دارند
III. استگانوگرافی (استتار)
IV. رعایت سایر مسایل امنیتی

رمزنگاری: همچنان که تکنولوژی برای فعالین اجتماعی و دیگر سازمان های تحت ریسک ابزار مهمتری می شود، ایمنی ارتباطات و اطلاعاتی که آن ها جمع آوری کرده اند نیز بیشتر در معرض خطر قرار می گیرد و همین امر است که بیش از پیش اهمیت رمزنگاری را برجسته می کند.

رمزگذاری چیست؟ هنر در هم ریختن اطلاعات به شیوه ای که تنها طرف مقابل قادر به خواندن آن باشد. یکی از حیاتی ترین حوزه های رمزگذاری، رمزگذاری ایمیل ها است. این امر بخصوص درباره افرادی صادق است که بدلیل فعالیتهای اجتماعی هدف شنود و تحت نظر هستند.

نکته ای که بیشتر کاربران اینترنت نمی دانند یا به آن توجه نمی کنند این است که وقتی داده ای (ایمیل، چت یا ...) را روی شبکه عمومی اینترنت می فرستیم، هر کسی با کمی تلاش می تواند آن را بخواند .ایمنی ارسال ایمیل، دقیقا به اندازه ایمنی ارسال کارت پستال است و رمزگذاری درست مانند یک پاکت محافظ برای نامه شما. رمزگذاری باعث می شود که متن پیام جز برای گیرنده برای کسی قابل دریافت نباشد. با اینکه ایمنی ۱۰۰٪ در ایمیل و اصولا کامپیوتر ممکن نیست، بازهم برداشتن هر قدمی برای ایمن کردن ارتباط بهتر از برنداشتن آن قدم است چرا که کار رقبا برای شنود اطلاعات شما با هر قدمی که برای رمزگذاری بردارید، یک قدم مشکل تر می شود. پس با اینکه استفاده از رمزگذاری ممکن است کمی وقت گیر باشد، ایمنی حاصل از آن ارزشمند است .

رمزگذاری نه تنها اطلاعات شما را به هنگام ارتباطات از شنود حفظ می کند که در عین حال شیوه ای برای اطمینان از هویت طرفین نیز هست. شما می توانید بیانیه صادر شده از طرف سازمان خود یا ایمیل یا هر سند دیگری را که می خواهید مردم مطمئن باشند که از طرف شما صادر شده است و سندی دروغین به نام شما نیست را به شکل دیجیتالی امضا کنید. اگر از امضاهای دیجیتالی برای مطالب سازمانتان استفاده نکنید، همیشه این امکان وجود دارد که کس دیگری سندی را به نام سازمان شما در دنیای دیجیتال پخش کند و همه تصور کنند که منبع آن سند شما بوده اید. این سند دروغین می تواند بیانیه ای باشد که مردم را دعوت به تجمع در نقطه ای کند و به دستگیری آن ها بیانجامد یا به اسم شما از مردم بخواهد کاری را بکنند که معمولا نمی کنند.

مبحث رمزنگاری را با مثال ساده ای ادامه می دهیم. فرض کنید شما در تهران هستید و قصد دارید نامه ای محرمانه به شخصی در شیراز بفرستید. نگرانی شما این است که کسی نتواند در مسیر تهران به شیراز به متن نامه شما دسترسی پیدا

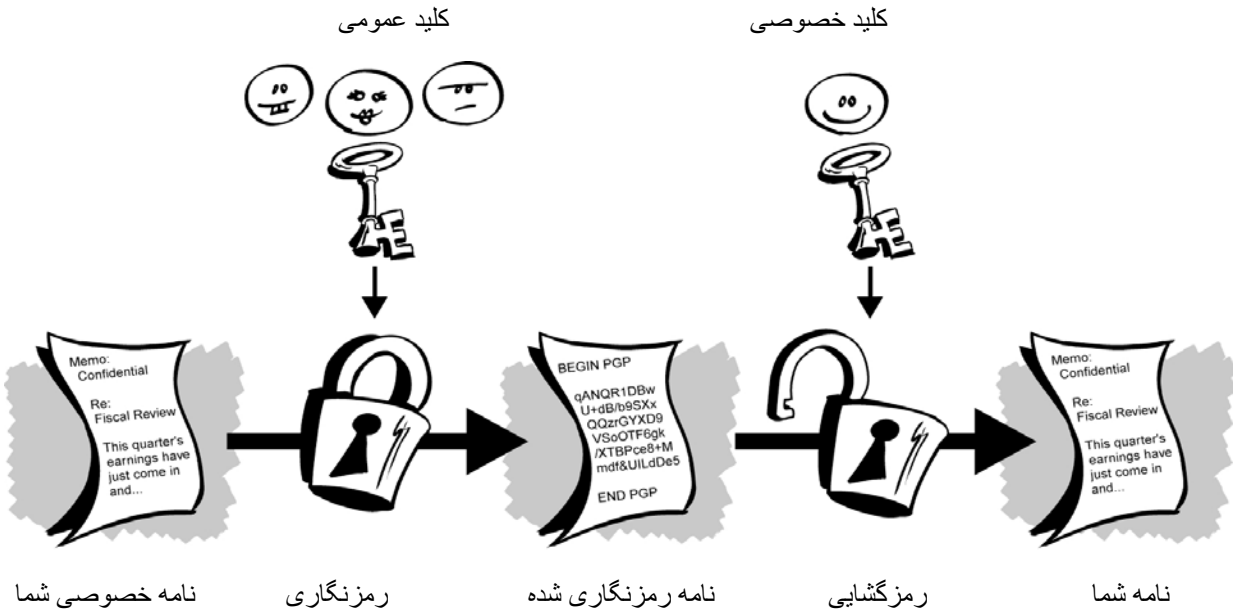
کند. بهتر این است که نامه خود را به زبانی بنویسید که فقط شما و گیرنده نامه به آن مسلط هستید. در این صورت حتی اگر نامه شما در بین راه توسط شخص دیگری نیز خوانده شود، آن شخص قادر به فهمیدن متن نامه خصوصی شما نخواهد بود.

در دنیای اینترنت وقتی که قصد فرستادن ایمیل دارید، ایمیل شما به صورت بسته ای از داده (اطلاعات) در می آید که به طرف مقصد و یا در این صورت گیرنده ایمیل شما فرستاده می شود. اطلاعات فرستاده شده قبل از رسیدن به مقصد از مسیرهای مختلفی می گذرند و همانطور که در مثال فرضی گفتیم دیگران در فاصله بین فرستنده و گیرنده قادر به دیدن اطلاعات فرستاده شده هستند.

2 نوع رمزنگاری وجود دارد: متقارن و نامتقارن

در روش متقارن اطلاعات توسط یک کلید رمزنگاری شده و توسط همان کلید رمزگشایی می شود. بعنوان مثال الفبای فارسی را بعنوان یک جدول در نظر گرفته و سپس یک حرف را با حرف دیگری درتعویض می کنیم. این قرارداد را به شخص گیرنده هم اطلاع داده و گیرنده می تواند بر اساس همان قرارداد نامه رمزنگاری شده را رمزگشایی کند. در این نوع رمزنگاری به این دلیل که تنها یک کلید وجود دارد و این کلید در دسترس هم فرستنده و هم گیرنده می باشد ریسک رمزگشایی توسط دیگران وجود دارد.

اما در روش نامتقارن 2 نوع کلید وجود دارد: کلیدی که برای رمزنگاری بکار می رود (کلید عمومی) و کلیدی که توسط آن رمزگشایی می شود (کلید خصوصی) و این دو کلید مکمل همدیگر هستند. هر فرد می‌تواند «کلید عمومی» و «خصوصی» منحصر به فرد خودش را داشته باشد و کلید عمومی را در اختیار همه قرار دهد، هرچه با کلید خصوصی رمز شود فقط با کلید عمومی کشف رمز و باز می شود. بدون داشتن کلید خصوصی امکان رمزگشایی نامه ای که توسط روش نامتقارن رمزنگاری شده است بسیار مشکل است. در واقع با داشتن بهترین روش‌ها حدود چند صد سال وقت لازم است تا یک رمز نامتقارن رایج بدون داشتن کلید خصوصی آن شکسته شود. در شکل زیر مراحل رمزنگاری در شیوه نامتقارن بنمایش گذاشته شده است.



مثالی برای رمزنگاری نامتقارن: برای نمونه اگر مریم بخواهد به کاوه نامه ای بفرستد یا بالعکس، باید هر دو نفر هم کلید هممومی داشته باشند و هم کلید خصوصی. برای ارسال نامه به کاوه باید مریم کلید عمومی کاوه را داشته باشد ، پس کاوه از طریقی مطمئن کلید عمومی مریم را دریافت کند واطلاعات خود را با این کلید رمز کرده و برای مریم ارسال می کند ، حالا فقط مریم است که می تواند اطلاعات رمز نگاری شده را ببیند چرا که کلید محرمانه یا خصوصی مربوطه در دستان کاوه است.

یکی از نرم افزارهایی که از روش نامتقارن برای رمزنگاری استفاده می کند برنامه PGP (Pretty Good Privacy) که برای رمزنگاری و امضای دیجیتال ایمیل بکار می رود. PGP سه قابلیت رمزنگاری، تصدیق هویت و دریافت بدون نقص امنیت اطلاعات شما را تامین می کند:

رمزنگاری : این قابلیت به شما کمک می کند تا اطلاعات خود را رمز کنید تا جز فردی که شما می خواهید شخص دیگری نتواند به محتوای آن دست پیدا کند.

تصدیق هویت: این قابلیت شما را قادر می سازد تا از هویت شخص فرستنده اطلاع پیدا کنید.
3. دریافت بی نقص:این قابلیت به شما کمک می کند تا از اصل بودن اطلاعات ارسالی کسب اطمینان کنید و اگر پلیس یا یک هکر در میانه ی راه اطلاعات شما را تغییر دهد بوسیله ی این قابلیت شما از این تغییرات مطلع خواهید شد.

نصب و استفاده از PGP شامل مراحل زیر می باشد:

1. نصب برنامه PGP
2. استخراج کلیدها
3. فرستادن کلید عمومی به دیگران
4. دریافت کلید عمومی از دیگران
5. ارسال و دریافت ایمیل از دیگران

برای نصب و استفاده از PGP می توانید از ویدیوی آموزشی که تهیه کرده ایم استفاده کنید. این ویدیو را می توانید از اینجا دریافت کنید.

II. **استفاده از ایمیل کلاینتهایی که امنیت بالایی دارند**: تمامی ایمیلها و لیست آدرس ایمیلهایی را که در outlook express دارید در هارد دیسک شما ثبت می کردد. توصیه می شود که از این برنامه استفاده نکنید. پیشنهاد ما این است که از برنامه تاندربرد که امنتر است استفاده کنید. تاندربرد را می توانید از اینجا دریافت کنید.

III. استگانوگرافی (استتار):

استگانوگرافی هنر مخفی کردن یک متن در متن دیگری است. یکی از روشهای استتار، قرار دادن یک متن در یک تصویر است. سپس می توانید این عکس را برای گیرنده بفرستید. در اینصورت حتی اگر این تصویر بدست پلیس بیفتد اطلاعات شما لو نخواهد رفت. برای استتار متون خود در تصاویر پیشنهاد می کنیم که از برنامه Hit Mail Privacy 4 Lite استفاده کنید زیرا قابلیت استتار متنی را در تصویر فراهم می کند. این برنامه مخفی کردن را با رمزگذاری های قوی ترکیب می کند تا ایمنی بیشتری ایجاد کند. می توانید از هر تصویری با هر مضمونی استفاده کنید. مثلا عکسی از طبیعت را انتخاب کرده و با کمک نرم افزار یاد شده متن پیام سری خود را در آن استتار کنید و این عکس را برای گیرنده بفرستید. این برنامه را می توانید از اینجا دریافت کنید. روش استتار روش بسیار مناسبی برای مبادله امن اطلاعات است و پیشنهاد می کنیم آن را بصورت روتین برای ارسال اطلاعات سری خویش استفاده کنید.

IV. رعایت سایر مسایل امنیتی:

- ✓ استفاده از Hushmail : یک سرویس ایمیل مبتنی بر وب است (یعنی باید از طریق مرورگر اینترنت به آن دسترسی پیدا کنید) که به شما اجازه می دهد با ایمنی بالایی، ایمیل بفرستید و دریافت کنید. پیام های هاشمیل و پیوست های آن ها با استفاده از استاندارد OpenPGP رمزگذاری می شوند. این باعث سطح بالایی از ایمنی برای کاربران سایت می شود. پیام ها قبل از ترک کامپیوتر شما رمزگذاری می شوند و تا وقتی به کامپیوتر مقابل نرسیده اند، جایی که در آن به شکل اتوماتیک رمزگشایی خواهند شد، برای کسی قابل درک نیسند. رمزگذاری نامه ها به سادگی یک کلیک کردن است. نکته: ۱) حداقل هر سه هفته یکبار باید به شناسه هاشمیل خود سر بزنید وگرنه بسته خواهد شد ۲) برای استفاده از ایمنی هاشمیل حتما باید گیرده شما هم از هاشمیل استفاده کند.

- ✓ برخی از کاربران این تصور را دارند که فایل های متن با انشعاب txt و یا فایل های گرافیکی (. bmp ,jpg, .gif) ایمن می باشند ولی همواره اینچنین نخواهد بود . انشعاب يك فايل می تواند جعل شود و مهاجمان از تنظیمات پیش فرض ویندوز که انشعاب فایل های متداول را نمایش نمی دهد، سوء استفاده نمایند . به عنوان نمونه ، فایل greatfile.jpg.exe که انشعاب واقعی آن مخفی است به صورت greatfile.jpg نمایش داده خواهد شد و کاربران فکر می کنند که فایل فوق يك فايل گرافیکی است ولی در واقع يك برنامه مخرب است. کاربران کامپیوتر می بایست صرفا" در مواردی که انتظار دریافت يك ایمیل به همراه ضمیمه مورد نظر را از يك منبع تائید شده و در آن زمان خاص دارند، اقدام به بازنمودن فایل های ضمیمه نمایند . حتی در صورتی که يك نامه الکترونیکی به همراه فایل ضمیمه ای را دریافت می نمائید که نسبت به هویت ارسال کننده آن هیچگونه تردیدی وجود ندارد ، این احتمال وجود خواهد داشت که آدرس فوق توسط مهاجمان جعل و یا توسط کامپیوتری آلوده به ویروس و بدون اطلاع صاحب آن ارسال شده باشد.

- ✓ ایمیلهایی را که دریافت می کنید یا برای دیگران می فرستید حتما از ایمیل خود حذف کنید. این به این دلیل است که عدم حذف ایمیلهای شما یک بانک اطلاعاتی را در صورت دسترسی دیگران به ایمیل شما فراهم می کند و اطلاعاتی غیر قابل انکار در اختیار بازجوها قرار می دهد. حتما ایمیلهای خود را از پوشه Inbox و Sent حذف کنید. اگر به هر دلیلی مایل به نگاهداری ایمیلهای خویش هستید، یک ایمیل آدرس دیگر را برای خود ثبت کنید، ایمیلی که کسی به غیر از شما از آن اطلاع ندارد. ایمیلهای خود را از آدرس اصلی به ایمیل دوم و محرمانه خود فوروارد کنید و حتما فراموش نکنید که ایمیلها را در پوشه Inbox و Sent حذف کنید.

- ✓ بعد از ورود به ایمیل و استفاده از آن بیاد داشته باشید که حتماً Sign Out کنید. ردپای شما در Cookies (کوکی ها) باقی می ماند و در صورتی که از ایمیل خاج نشوید، شخص دیگری می تواند ایمیلهای شما را بخواند.

- ✓ استفاده از پسوردهای امن: پسوردها تنها در صورتی دسترسی غریبه ها به منابع موجود را محدود می کند که حدس زدن آن به سادگی امکان پذیر نباشد. پسوردهای خود را در اختیار دیگران قرار ندهید و از یک پسورد در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت. قانون طلایی برای انتخاب گذرواژه شامل موارد زیر است:گذرواژه باید حداقل شامل 8 حرف بوده، حتی الامکان کلمه ای بی معنا باشد. در انتخاب این کلمه اگر از حروف کوچک، بزرگ و اعداد استفاده شود ضریب امنیت بالا تر خواهد رفت. سعی کنید به صورت منظم پسورد قبلی را عوض نمایید. هرگز از پسوردهایی که حدس زدن آنها آسان باشند استفاد نکنید مثلا استفاده از نام یکی از بستگان یا تاریخ تولد.

- ✓ اگر در متن ایمیل دریافتی لینکی قرار دارد که از شما دعوت شده است که با استفاده از آن به ایمیل خود وارد شوید، از انجام این کار خودداری کنید زیرا این نوع ترفندها برای بدست آوردن یوزر و پسورئ شما می باشد و fake login نامیده می شود.

- ✓ اگر در ایمیل شما لینکی قرار دارد که پس از ورود به آن قادر به خواندن متون صفحه نمی باشید اما لینک دانلود فونت وجود دارد، بلافاصله صفحه را ببندید و از دانلود فونت که به احتمال زیاد تروجان می باشد خودداری کنید.

افزایش امنیت کلاینتهای چت

برای افزایش امنیت خود در چت پیشنهاد می کنیم مطابق دستورات زیر عمل کنید.

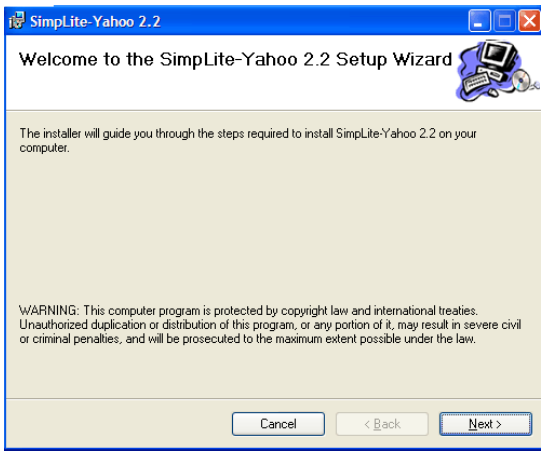
I. استفاده از نرم افزارهایی که یاهو مسنجر و گوگل تاک را امنتر می کنند
II. استفاده از چت کلاینتهایی که امنیت بیشتری دارند
III. رعایت سایر مسایل امنیتی

I. افزایش امنیت یاهو مسنجر و گوگل تاک: برای افزایش امنیت یاهو مسنجر و گوگل تاک پیشنهاد می کنیم از برنامه های ویژه ای که برای رمز کردن چت وجود دارند، استفاده کنید. هم برای رمز کردن چت کتبی و هم برای رمز کردن مکالمات شفاهی. برای رمز کردن یاهو مسنجر، گوگل تاک میتوانید از برنامه Simp استفاده کنید. برای استفاده از رمزنگاری باید هر دو طرف مکالمه این نرم افزار را نصب و تنظیم کرده باشند.

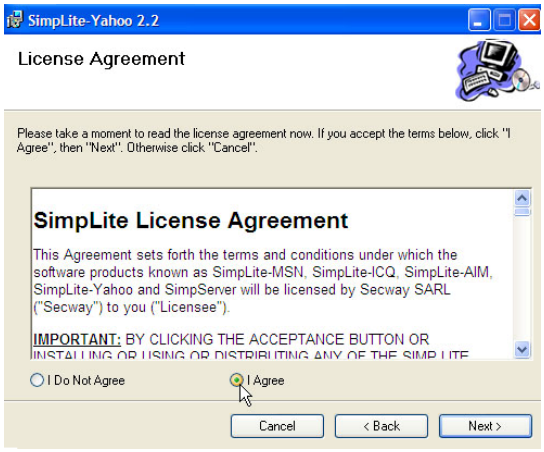
یاهو مسنجر: ویدیو آموزشی برنامه برنامه SimpLite برای یاهو را از اینجا دریافت کنید. همچنین می توانید از راهنمای زیر استفاده کنید.

- ✓ برنامه SimpLite برای یاهو را از اینجا دریافت کنید.
- ✓ مطابق تصاویر زیر این برنامه را نصب کنید.

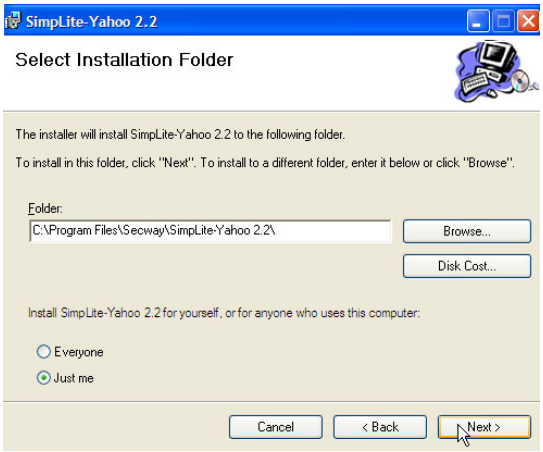
1



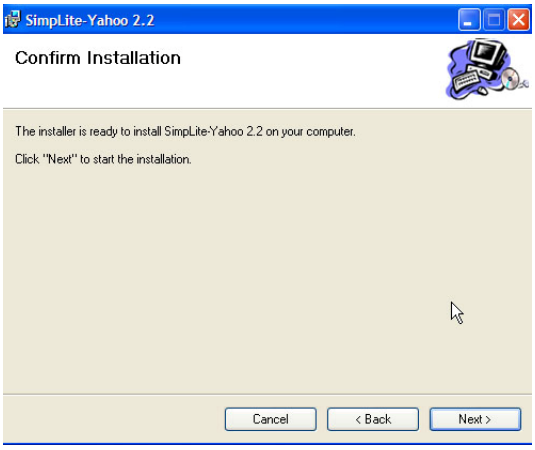
2



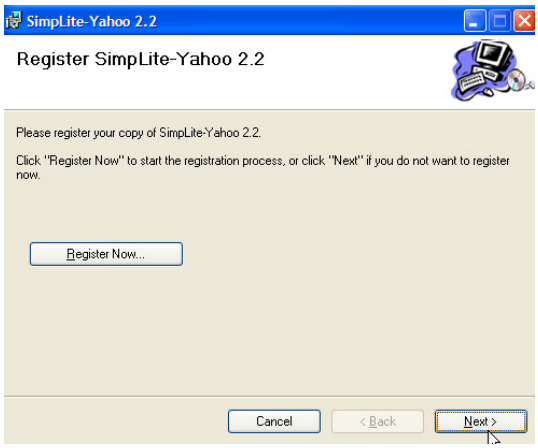
3



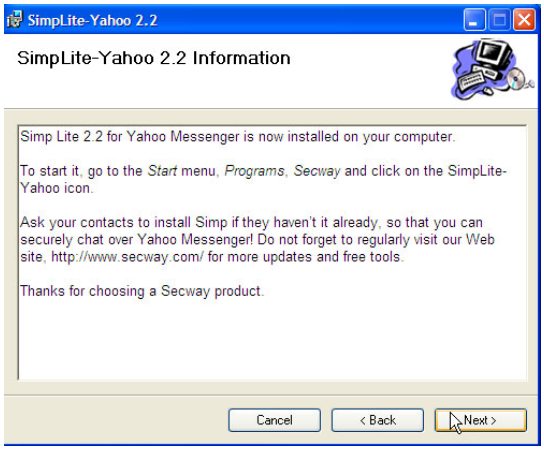
4



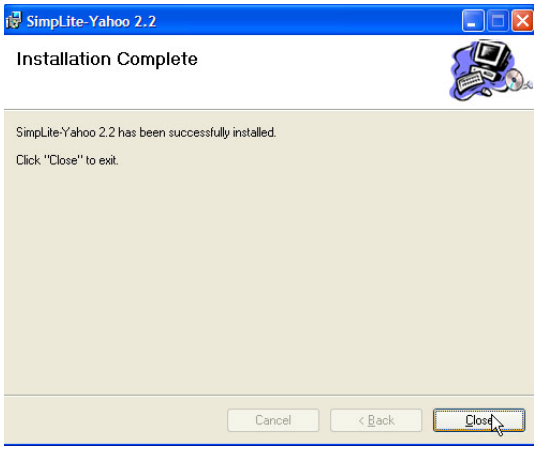
5


SimpLite-Yahoo 2.2
Register SimpLite-Yahoo 2.2
Please register your copy of SimpLite-Yahoo 2.2.
Click "Register Now" to start the registration process, or click "Next" if you do not want to register now.
Register Now...
Cancel
< Back
Next >

6


SimpLite-Yahoo 2.2
SimpLite-Yahoo 2.2 Information
Simp Lite 2.2 for Yahoo Messenger is now installed on your computer.
To start it, go to the Start menu, Programs, Secway and click on the SimpLite-Yahoo icon.
Ask your contacts to install Simp if they haven't it already, so that you can securely chat over Yahoo Messenger! Do not forget to regularly visit our Web site, http://www.secway.com/ for more updates and free tools.
Thanks for choosing a Secway product.
Cancel
< Back
Next >

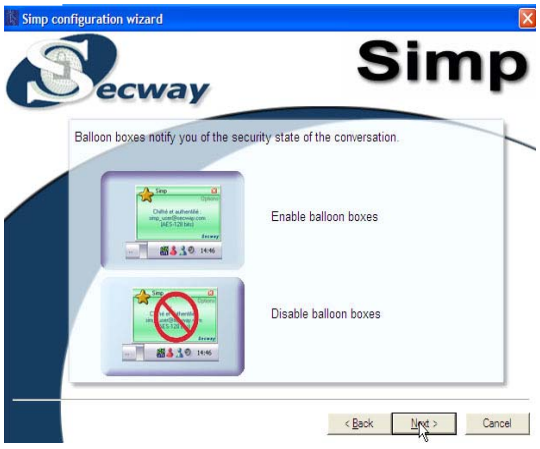
7


SimpLite-Yahoo 2.2
Installation Complete
SimpLite-Yahoo 2.2 has been successfully installed.
Click "Close" to exit.
Cancel
< Back
Close

8


Simp configuration wizard
Secway
Simp
Welcome to the Simp configuration wizard!
This wizard will help you configure Simp and your messaging clients.
On each screen, you will be prompted to enable or disable Simp options, or configure popular messaging clients. To go back to the previous screen, click "Back"; previous options won't be modified.
Changes are only applied after validating the final screen. You can discard modifications at any time by clicking "Cancel"; current configuration parameters would be kept.
Please click "Next" to start.
< Back
Next >
Cancel

9

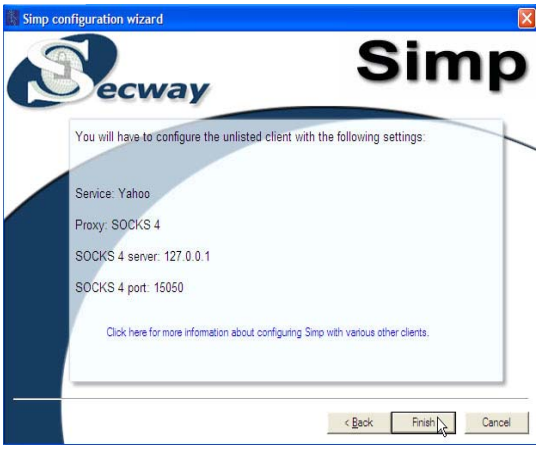

Simp configuration wizard
Secway
Simp
Balloon boxes notify you of the security state of the conversation.
Enable balloon boxes
Disable balloon boxes
< Back
Next >
Cancel

10


Simp configuration wizard
Secway
Simp
Simp needs to know what kind of Internet connection you use. If you don't know, Simp will do its best to detect it.
I don't know
Direct connection
SOCKS 4 proxy
SOCKS 5 proxy
HTTP proxy
< Back
Next >
Cancel

11

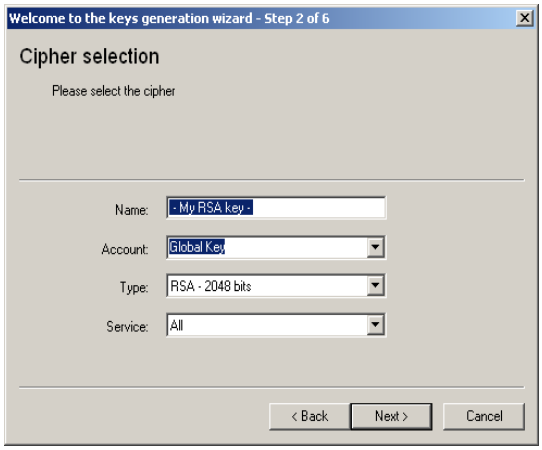
12



✓ پس از نصب لازم است که کلیدهای لازم را بسازیم. بلافاصله پس از اتمام نصب صفحه ساخت کلیدها باز می شود. برای ساختن کلیدها مطابق تصاویر زیر عمل کنید.

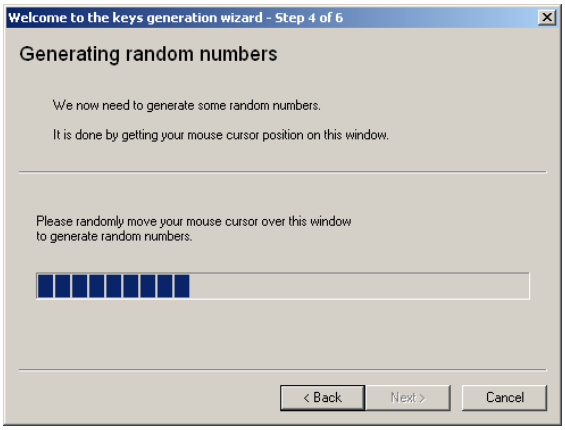
1

2

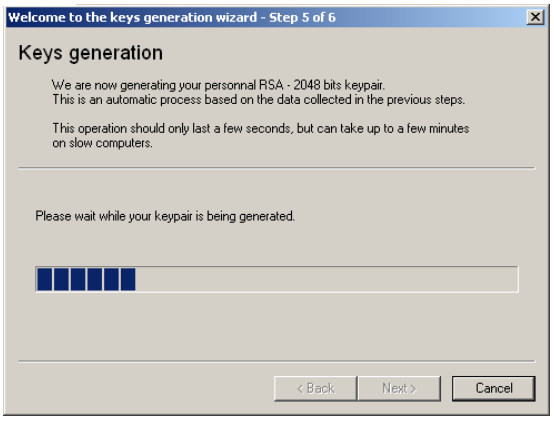


3

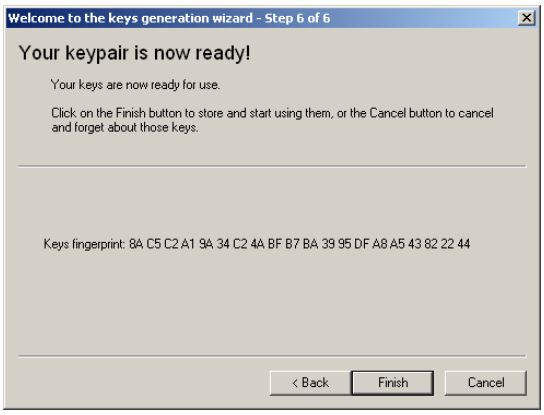
4



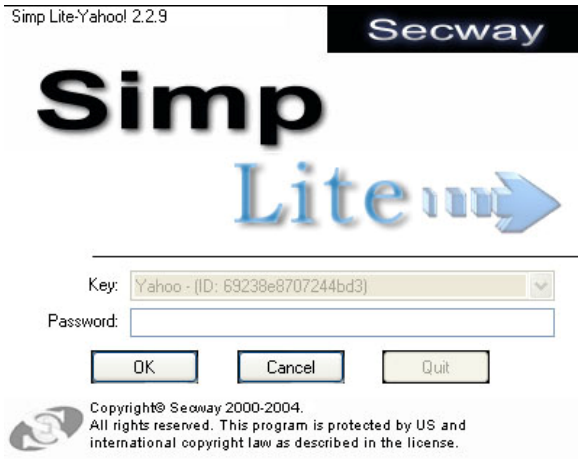
5



6



✓ پس از نصب و ساختن کلید می توانید لاگین کنید. برای ورود پسوردی را که در خلال ساختن کلیدها مورد استفاده قرار دادی دی فیلد پسورد وارد کنید. تصویر صفحه لاگین را می توانید اینجا ببینید:



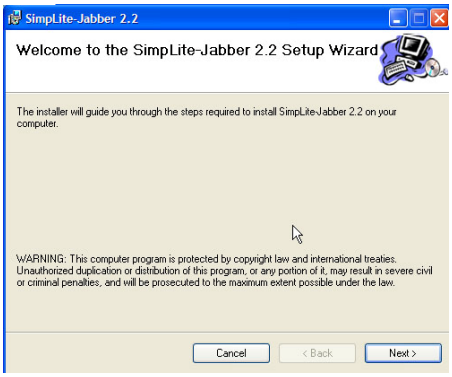
✓ بعد از این وارد یاهو مسنجر شوید. برنامه سیمپ چتهای شما را بطور اتوماتیک شناسایی خواهد کرد. اگر بار اول با کسی که سیمپ دارد مکالمه ای را شروع کنید باید کلید عمومی آن شخص را مورد تایید قرار دهید. اینکار فقط یکبار لازم است و در چتهای آینده سیمپ کلید وارد شده را به یاد خواهد آورد. در هنگام چت سیمپ به شما وضعیت رمزنگاری را خواهد گفت. به تصویر زیر نگاه کنید:

تنها مکالماتی که رنگ سبز دارد امنیت آن از طریق سیمپ تامین شده است. اگر رنگ مقابل آی دی قرمز است مطمئن شوید که طرف مقابل شما هم سیمپ دارد زیرا برای استفاده از سیمپ هر دو طرف باید سیمپ را نصب و تنظیم کرده باشند.

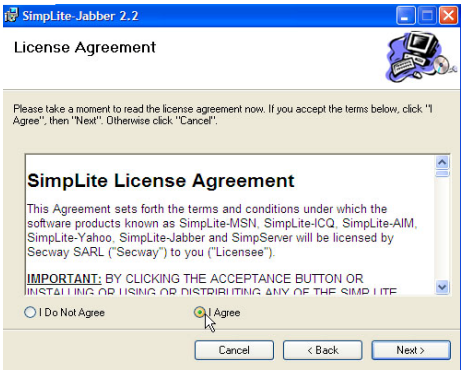
گوگل تاک: ویدیو آموزشی برنامه SimpLite برای گوگل تاک را از اینجا دریافت کنید. همچنین می توانید از راهنمای زیر استفاده کنید.

- ✓ برنامه SimpLite برای گوگل تاک را از اینجا دریافت کنید.
- ✓ مطابق تصاویر زیر این برنامه را نصب کنید.

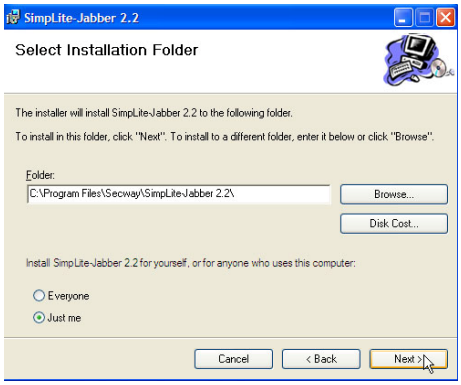
1



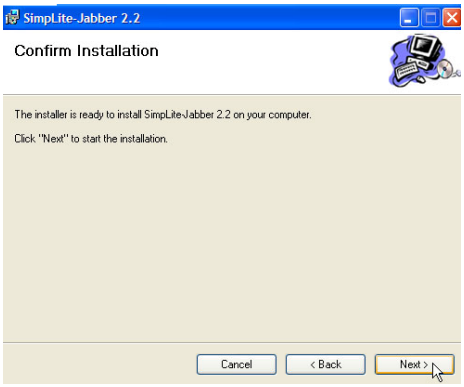
2



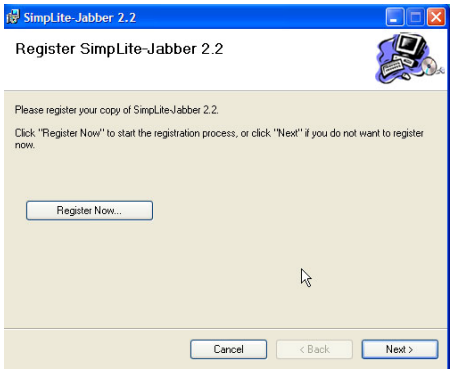
3



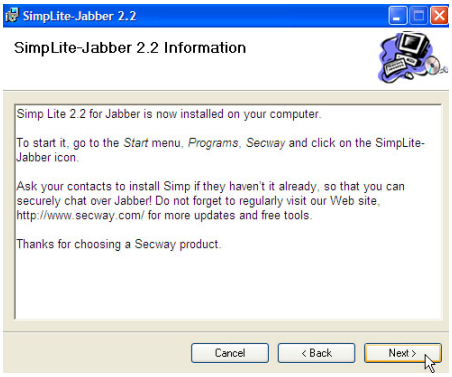
4



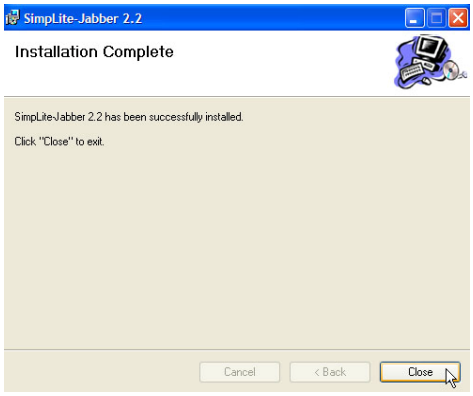
5



6



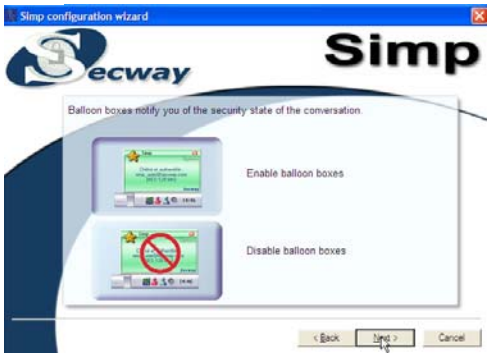
7


SimpLite-Jabber 2.2
Installation Complete
SimpLite-Jabber 2.2 has been successfully installed.
Click "Close" to exit.
Cancel
< Back
Close

8


Simp configuration wizard
Simp
Welcome to the Simp configuration wizard!
This wizard will help you configure Simp and your messaging clients.
On each screen, you will be prompted to enable or disable Simp options, or configure popular messaging clients. To go back to the previous screen, click "Back"; previous options won't be modified.
Changes are only applied after validating the final screen. You can discard modifications at any time by clicking "Cancel"; current configuration parameters would be kept.
Please click "Next" to start.
< Back
Next >
Cancel

9


Simp configuration wizard
Simp
Balloon boxes notify you of the security state of the conversation.
Enable balloon boxes
Disable balloon boxes
< Back
Next >
Cancel

10


Simp configuration wizard
Simp
Simp needs to know what kind of Internet connection you use. If you don't know, Simp will do its best to detect it.
I don't know
Direct connection
SOCKS 4 proxy
SOCKS 5 proxy
HTTP proxy
< Back
Next >
Cancel

11


Simp configuration wizard
Simp
Please choose which IM client application you are using:
Google Talk
Trillian
Gaim
Unlisted Jabber client
< Back
Finish
Cancel

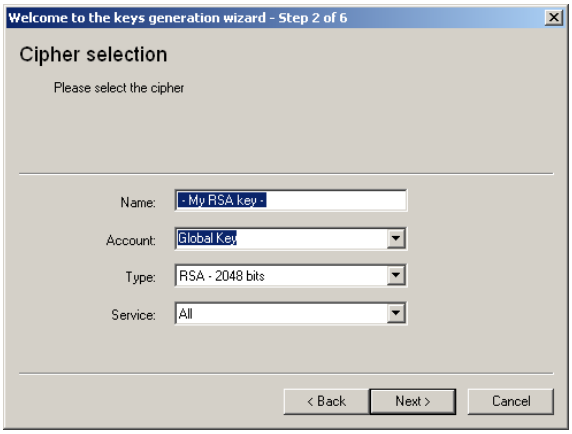
12


Simp configuration wizard
Simp
You will have to configure the unlisted client with the following settings:
Service: Yahoo
Proxy: SOCKS 4
SOCKS 4 server: 127.0.0.1
SOCKS 4 port: 15050
Click here for more information about configuring Simp with various other clients.
< Back
Finish
Cancel

✓ پس از نصب لازم است که کلیدهای لازم را بسازیم. بلافاصله پس از اتمام نصب صفحه ساخت کلیدها باز می شود. برای ساختن کلیدها مطابق تصاویر زیر عمل کنید.

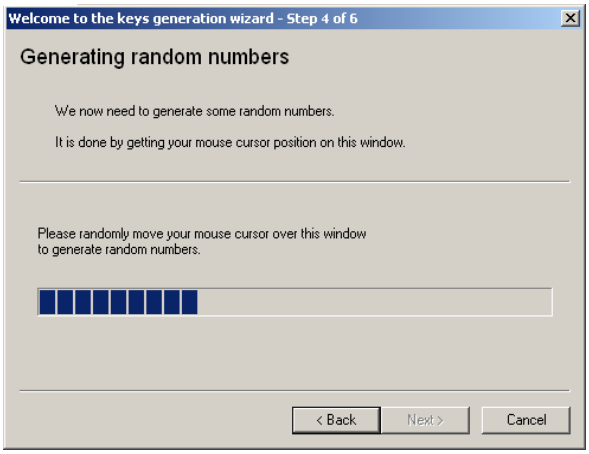
1

2

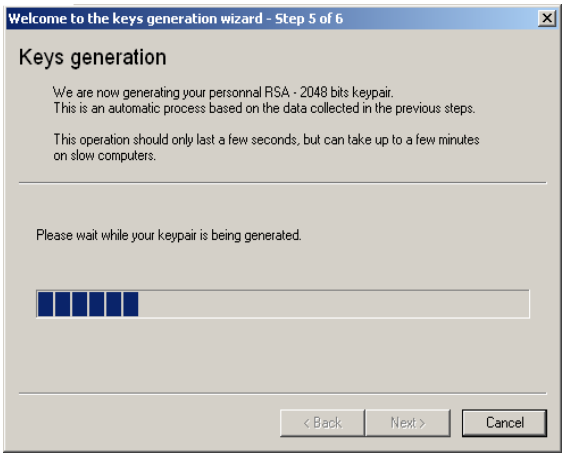


3

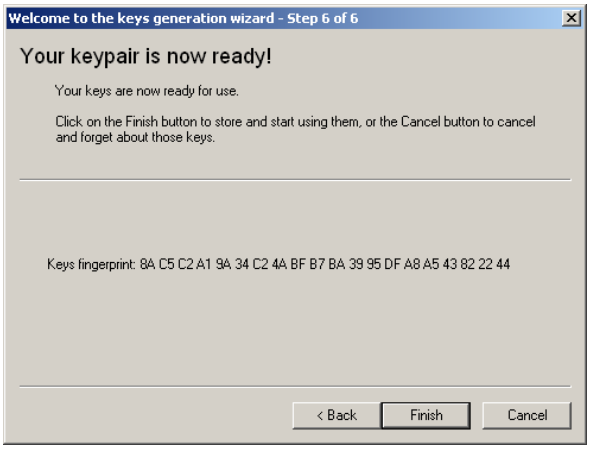
4



5



6



- ✓ پس از نصب و ساختن کلید می توانید لاگین کنید. برای ورود پسوردی را که در خلال ساختن کلیدها مورد استفاده قرار دادی دی فیلد پسورد وارد کنید. بعد از این وارد گوگل تاک بشوید. برنامه سیمپ چتهای شما را بطور اتوماتیک شناسایی خواهد کرد. اگر بار اول با کسی که سیمپ دارد مکالمه ای را شروع کنید باید کلید عمومی آن شخص را مورد تایید قرار دهید. اینکار فقط یکبار لازم است و در چتهای آینده سیمپ کلید وارد شده را به یاد خواهد آورد. در هنگام چت سیمپ به شما وضعیت رمزنگاری را خواهد گفت. به تصویر زیر نگاه کنید:

تنها مکالماتی که رنگ سبز دارد امنیت آن از طریق سیمپ تامین شده است. اگر رنگ مقابل آی دی قرمز است مطمئن شوید که طرف مقابل شما هم سیمپ دارد زیرا برای استفاده از سیمپ هر دو طرف باید سیمپ را نصب و تنظیم کرده باشند.

II. دیواره آتش یاهو مسنجر را فعال کنید: در یاهو مسنجر جدید براي مقابله با هك تنظيمات مناسب جدي را در اختيار قرار داده است .براي فعال كردن ديرواه آتش بدين ترتيب عمل كنيد: پس از ورود به یاهو مسنجر گزینه Messenger را انتخاب کنید و روی گزینه Preferences کلیک کنید. در صفحه ای که باز می شود روی گزینه Coonection کلیک کنید و Firewall with no proxies را انتخاب کنید. برای ثبت تغییرات لازم است که از یاهو مسنجر خارج شده و دوباره وارد شوید. اکنون یاهو مسنجر شما داراي ديواره آتش می باشد.

III. **استفاده از چت کلاینتهایی که امنیت بیشتری دارند**

- ✓ Pidgin یک برنامه چت اینترنتی چند پروتکلی است. یکی از مزیت های اصلی آن این است که می توانید از آن برای دسترسی به شناسه های اکثر سیستم های چت مرسوم همچون (ICQ، MSN، Yahoo! ،IRC ،Jabber) استفاده کنید. کاربران پیدگین می توانند همزمان وارد چندین سیستم چت اینترنتی شوند. یعنی می توانید همزمان در حال چت با دوستانتان در یاهو باشید و با دوستی در گوگل تاک صحبت کنید. برنامه پیدگین را می توانید از اینجا دریافت کنید. یک مزیت دیگر پیدگین این است که پلاگینی برای آن وجود دارد که به شما اجازه می دهد با رمزگذاری مکالمات ، ایمنی ارتباط خود را بالا ببرید. این پلاگین را می توانید از اینجا دریافت کنید و از طریق tools>plugins فعالش کنید و سپس امنیت هر بار گفتگویتان را با کلیک کردن بر روی آیکون قفل تضمین کنید.

- ✓ برنامه سکایپ هم امنیت بالاتری به نسبت یاهو مسنجر و گوگل تاک دارد. این برنامه را می توانید از اینجا دریافت کنید.

III. **رعایت سایر مسایل امنیتی**: اگر مسایل ایمنی را رعایت نکنید پلیس قادر به دسترسی به متن چتهایی شما خواهد بود. یاهو مسنجر شاید یکی از نرم افزارهایی باشد که به دلیل تبلیغات زیاد آن در میان کاربرانی که به تازگی با کامپیوتر آشنا شده اند مقبول و مورد استفاده است .فرض کنید شما در حال چت با دوستتان در یاهو مسنجر هستید، فکر می کنید پس از پایان چت و خروج از یاهو مسنجر چه اطلاعاتی از شما بروی سیستم باقی می ماند؟ شاید فکر می کنید هیچ اطلاعاتی و یا حداکثر آی دی شما و دوستتان بروی سیستم باقی می ماند. اما در بیشتر گفتگوهایی که با استفاده از یاهو مسنجر صورت می گیرد، آی دی شما و طرف مقابلتان و از همه مهمتر متن کامل چت هایتان بروی سیستم باقی می

ماند. باقی ماندن این حجم از اطلاعات کاملا شخصی ، حریم خصوصی شما را شدیدا به خطر می اندازد و پلیس با نرم افزارهایی قادر به دسترسی به اطلاعات خصوصی شما خواهد بود.

- مطلقا از آی‌دی های شناخته شده ای میلی و یا چت برای رد و بدل اطلاعات و چت در مورد مسائلی که نمیخواهید پلیس از آنها مطلع شود استفاده نکنید .بیاد داشته باشید که ارسال ای میل از آدرس های شناخته شده، ارسال ای میل به آدرس های شناخته شده، و چت آی‌دی های شناخته شده صد در صد توسط پلیس کنترل میشوند.

- حذف اطلاعات از ریجستری: بخش اعظم اطلاعات باقی مانده از مکالمات شما در ریجستری ویندوز ثبت خواهد شد و باید پس از اتمام چت از سیستم پاک شود تا اطلاعات شما همچنان محفوظ باقی بماند. علاوه بر آن، این مسیر در رجیستری نیز حاوی ID های شماست که برای چت از ان استفاده کرده اید:

HKEY_CURRENT_USER\Software\yahoo\pager\profiles

حذف این مسیر پس از اتمام چت نیز توصیه می شود. برای حذف این اطلاعات محرمانه مراحل زیر را دنبال کنید:

- ✓ ابتدا از منوی Start گزینه Run… را انتخاب کنید
- ✓ سپس regedit را تایپ کنید
- ✓ Registry editor باز می شود. پاک نمودن ID های خود با ورود به مسیر رجیستری بالا پاک نمودن پوشه Profiles بعد از هر بار چت در مسیری که نرم افزار یاهو مسنجر نصب شده است.

- فراموش نکنید که حتما پس از اتمام چت یاهو مسنجر را کامل ببندید و sign out کنید

- از ثبت متن مکالمات خویش در آرشیو خودداری کنید. برای انجام این کار از منوی بالا گزینه Messenger را انتخاب کرده و سپس روی Preferences کلیک کنید. سپس از منوی سمت چپ Archive را انتخاب کنید. از گزینه های سمت راست No, do not save any of my messages و همچنین No, do not save my call history را انتخاب کرده و سپس روی Ok کلیک کنید تا تغیرات مورد نظر ثبت گردد.

- دسترسی دیگران را به دوربین خویش محدود کنید. برای انجام اینکار در منوی Preferences روی Webcam کلیک کنید و گزینه Always ask for my permission را انتخاب کنید.

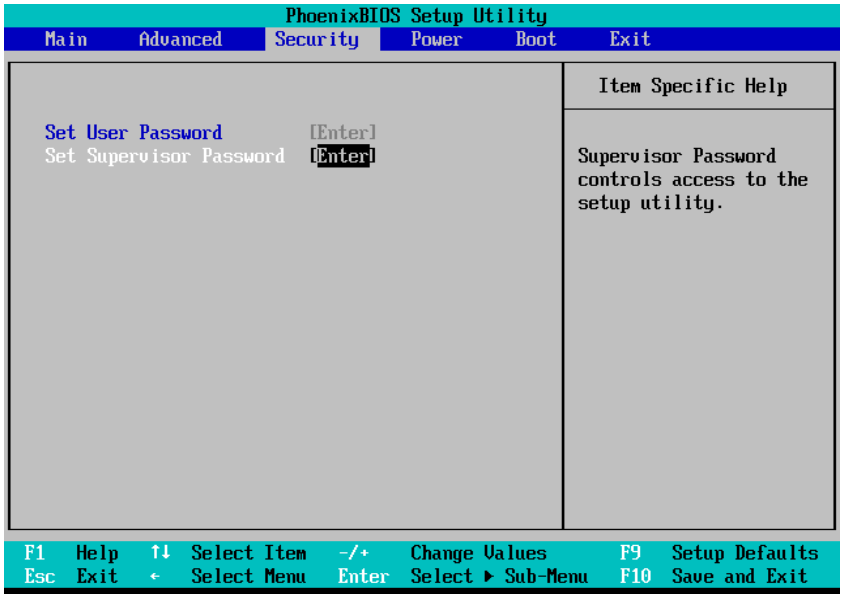
- در هنگام چت کردن از کسي فايلي دريافت نكنيد و اگر لازم است که این کار را بکنید، فایل دریافتی را با استفاده از آنتی ویروس اسکن کنید.

جلوگیری از سرقت اطلاعات شما از طریق دسترسی فیزیکی

حتی اگر کامپیوتر شما کاملا امن باشد و تمامی توصیه های امنیتی را رعایت کرده باشید هنوز این امکان برای پلیس وجود دارد که به فایلهای شما دسترسی پیدا کند و این از طریق دسترسی فیزیکی به کامپیوتر شما است. با استفاده از لایو سیدی که شامل سیستم عامل قابل حمل است می توان به آسانی به فایلهای موجود در ویندوز دسترسی پیدا کرد. برای جلوگیری از استفاده از این حفره امنیتی 3 راه را به شما پیشنهاد می کنیم:

1. پسورد گذاری برای Bios : برای جلوگیری از انجام تغییرات در Bios و بوت شدن کامپیوتر شما با استفاده از لایو سیدی می توانید Bios را پسورد گذاری کنید .اولین برنامه ای است که پس از روشن کردن کامپیوتر شروع بکار می کند. با پسورد گذاری می توانید دسترسی به Bios را محدود کنید. برای انجام اینکار مطابق راهنمای زیر عمل کنید:

کامپیوترتان را روشن کنید. پیامی مانند Hit the <DEL> key to enter the BIOS setup program در اسکرین ظاهر می شود .پس از فشار دادن دکمه delete صفحه ای مانند منوی زیر باز می شود. در اینجا فقط می توانید از کیبورد استفاده کنید و ماوس قابل استفاده نیست. با استفاده از فلشهای کیبورد به قسمت Security بروید و Set Supervisor Passwordرا انتخاب کرده و روی Enter کلیک کنید. در اینجا پسوردی مناسب و قوی را انتخاب کنید سپس به قسمت Exitرفته و تغییرات را ذخیره کنید و از صفحه تنظیمات خارج شوید. ثبت تغییرات را همچنین می توانید با فشردن دکمه F10انجام دهید.



2. رمزنگاری هارد دیسک :بهترین راه برای جلوگیری از دستیابی پلیس به اطلاعات ثبت شده شما روی هارد دیسک می باشد .حتی اگر پلیس به هارد درایو شما دسترسی پیدا کند قادر به خواندن فایلهای شما نیست زیرا رمزنگاری شده است. نرم افزارهای متعددی در این ضمینه وجود دارند و پیشنهاد ما این است که برنامه رایگان و عالی TrueCryptرا که برای برای کدگذاری (Encrypt) کردن اطلاعات کامپیوتر مناسب است را استفاده کنید .از ویژگی های خوب این برنامه می توان به داشتن نسخه قابل حمل (Portable) ، و سرعت خوب آن اشاره نمود. این برنامه را می توانید از اینجا دریافت کنید.
3. از کار انداختن پورتهای USB : هر فردی میتواند با وصل کردن فلش خود به USB پورت به راحتی اطلاعات موجود روی هارد سیستم را منتقل کند. برای حفظ امنیت اطلاعات ، بسیاری در پی یافتن راهی برای جلوگیری از

انتقال اطلاعات به داخل فلش دیسک ها هستند. در این ترفند قصد داریم روشي را به سادگی و از طریق رجیستری ویندوز معرفي کنیم که با بهره گیری از آن میتوانید کپی یا انتقال اطلاعات به داخل فلش دیسک های وصل شده به USBرا کاملاً غیر ممکن نمایید .بدین منظور به مسیر زیر بروید :

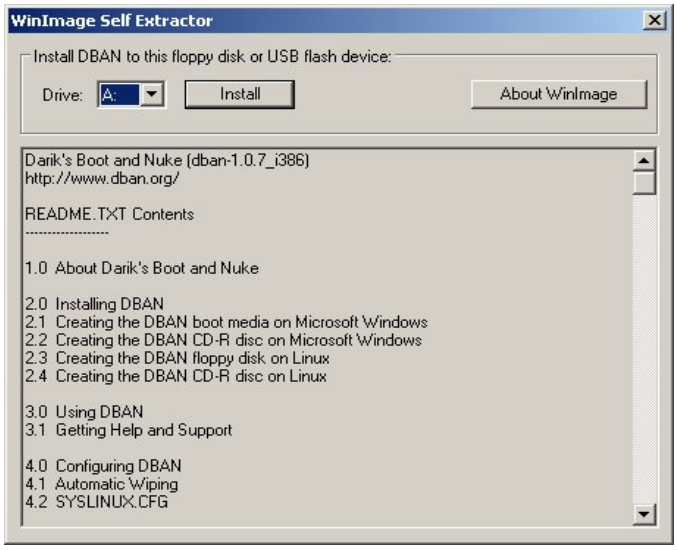
ابتدا از منوی Start گزینه ...Run را انتخاب کنید
سپس regedit را تایپ کنید
Registry editor باز می شود .سپس به این مسیر بروید :
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control

در ادامه روی کلید Control راست کلیک نموده و از New روي Key کلیک کنید. نام کلید جدید را StorageDevicePolicies قرار دهید.

اکنون اینبار روي کلید StorageDevicePolicies راست کلیک کنید و از منوي New روي DWORD Value کلیک کنید. نام مقدار جدید ساخته شده را writeProtect قرار دهید .حال روي writeProtect راست کلیک کنید و Modify را انتخاب نمایید .در قسمت Value Data عدد 0 را به 1 تغییر دهید و سپس OK کنید .اکنون رجیستری را ببندید و سیستم را ریستارت کنید .از این پس اگر بخواهیم اطلاعاتي را به یک حافظه فلش یا هر نوع حافظه همراه مانند Mp3 player ها منتقل کنید با پیغام خطا خواهیم شد .لازم به ذکر است برای بازگشت به حالت قبلي کافی است عدد 1 را مجدد به 0 تغییر دهید.

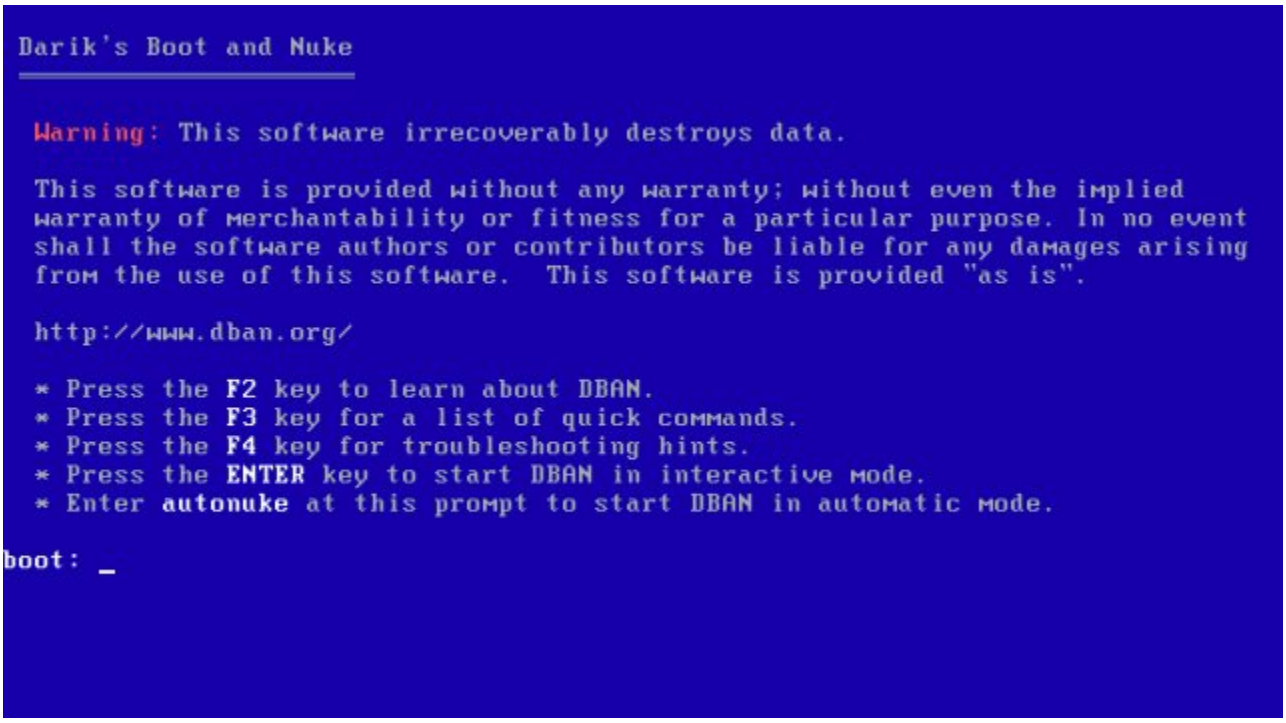
از بین بردن سریع هارد درایو در صورت احتمال دستگیری

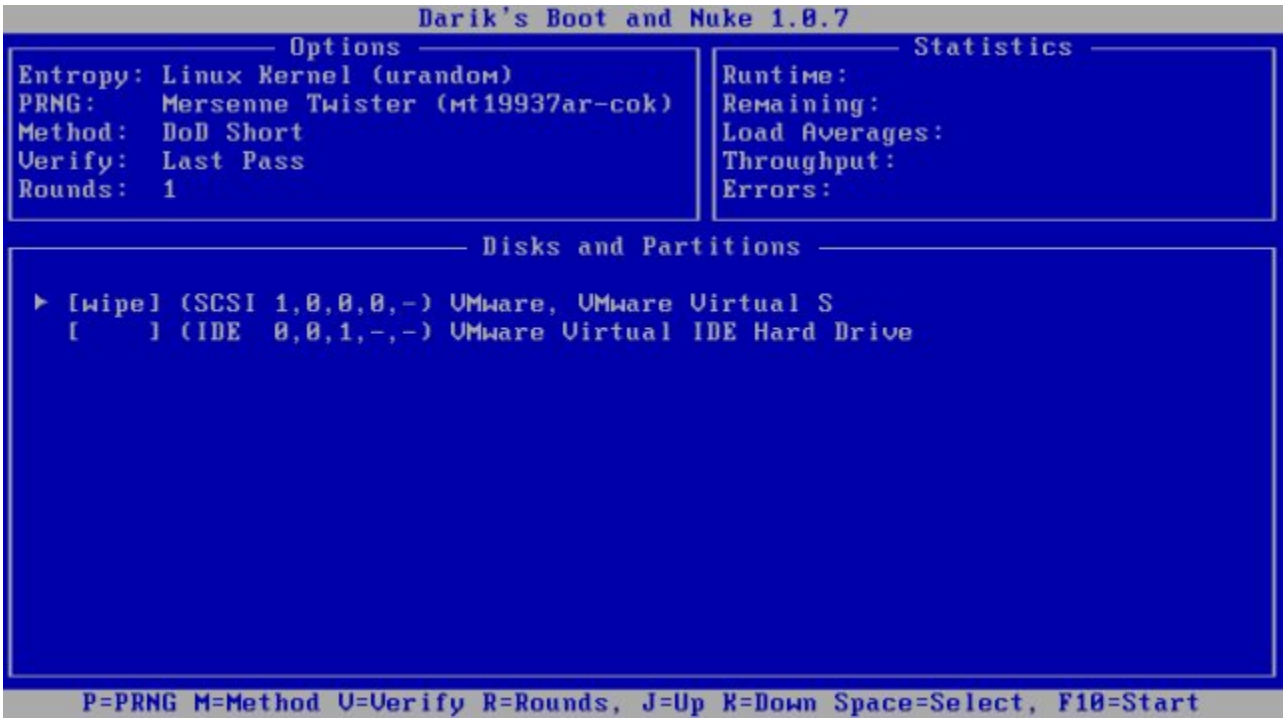
اگر به هر دلیلی احتمال می دهید که در معرض دستگیری قرار دارید و مدارکی در کامپیوتر شما است که پلیس از آن می تواند بر علیه شما استفاده می کند مطمئن ترین و سریعترین راه این است که هارد درایو را از بین ببرید. برای از بین بردن هارد درایو می توانید از 2 روش صدمه فیزیکی یا استفاده از نرم افزارهایی که اطلاعات را پاک می کنند استفاده کنید . صدمه فیزیکی روش خوبی است اما احتمال این وجود دارد که درایو کاملا از بین نرفته باشد. اگر برای صدمه فیزیکی وقت ندارید و به موفقیت آن اطمینان ندارید پیشنهاد می کنیم که از نرم افزار DBAN (Darik's Boot and Nuke)برای پاک کردن هارد درایو استفاده کنید .بیاد داشته باشید که قبل از اجرای این نرم افزار برنامه آنتی ویروس و دیواره آتش را غیر فعال کنید. این برنامه شروع به حذف سیستم عامل و تمامی فایلهای موجود در کامپیوتر شما به شیوه غیر قابل برگشتی خواهد کرد .برای نصب و استفاده از این برنامه مطابق راهنمای زیر عمل کنید:

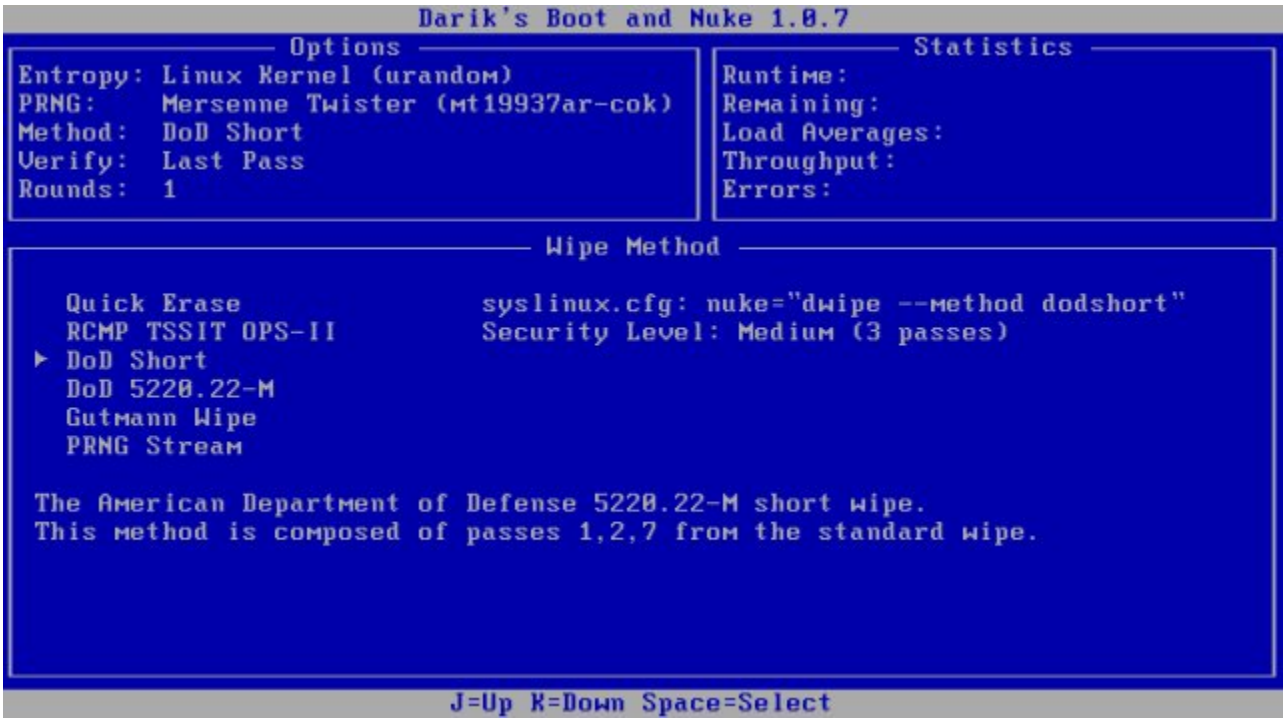


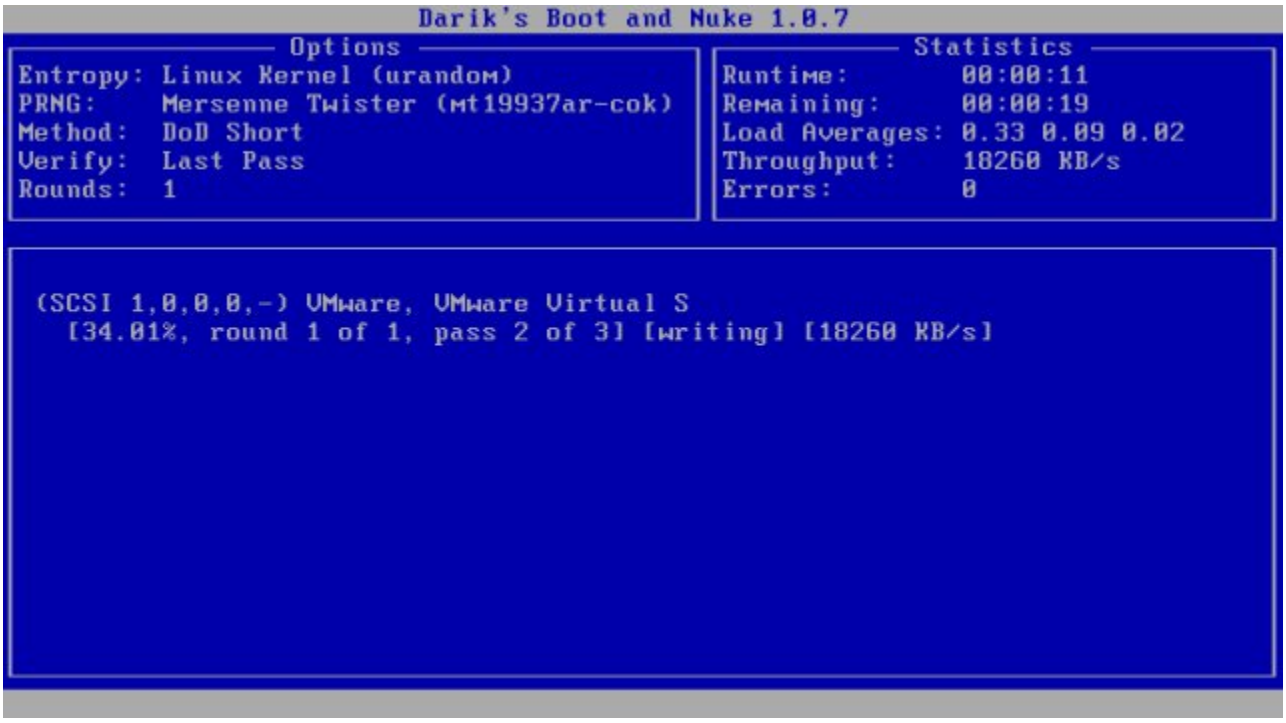
1. نصب :ابتدا نرم افزار DBAN را از اینجا دریافت کنید .برای دانلود این گزینه را انتخاب کنید for floppy disks and USB flash drives : .سپس یک دیسک فلاپی یا فلش به کامپیوترتان وصل کنید و روی فایل دانلود شده دو بار کلیک کنید تا برنامه روی فلاپی یا فلش نصب شود.

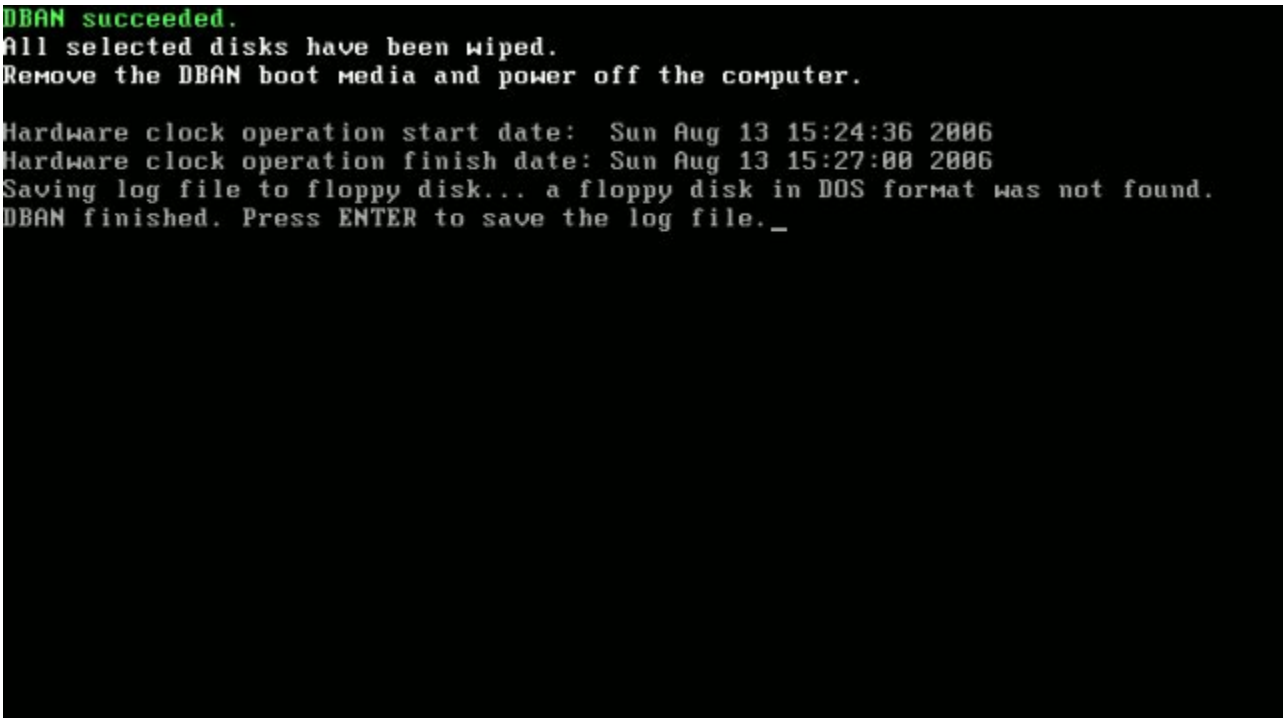
2. پاک کردن هارد درایو: دیسک فلاپی یا فلش را به کامپیوترتان وصل کنید و آن را ریستارت کنید. سپس طی مراحل زیر هارد درایو را به طور برگشت ناپذیری پاک کنید.






Darik's Boot and Nuke 1.0.7
Options
Entropy: Linux Kernel (urandom)
PRNG: Mersenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
Statistics
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:
Wipe Method
Quick Erase
RCMP TSSIT OPS-II
DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream
syslinux.cfg: nuke="dwipe --method dodshort"
Security Level: Medium (3 passes)
The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.
J=Up K=Down Space=Select


Darik's Boot and Nuke 1.0.7
Options
Entropy: Linux Kernel (urandom)
PRNG: Mersenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
Statistics
Runtime: 00:00:11
Remaining: 00:00:19
Load Averages: 0.33 0.09 0.02
Throughput: 18260 KB/s
Errors: 0
(SCSI 1,0,0,0,-) VMware, VMware Virtual S
[34.01%, round 1 of 1, pass 2 of 3] [writing] [18260 KB/s]


DBAN succeeded.
All selected disks have been wiped.
Remove the DBAN boot media and power off the computer.
Hardware clock operation start date: Sun Aug 13 15:24:36 2006
Hardware clock operation finish date: Sun Aug 13 15:27:00 2006
Saving log file to floppy disk... a floppy disk in DOS format was not found.
DBAN finished. Press ENTER to save the log file._

پایان