# راهنمای امنیت رایانه ای برای ایران

(نسخه ۰,۰,۳  شهریور ۱۳۸۸)



## آشنایی با این راهنما

هدف این راهنما صرفا افزایش آگاهی عمومی در مورد خطرات و راه های رفع آنها در محیط اینترنت و رایانه شخصی است. موارد زیر مورد بررسی قرار می گیرند:

1. آشنایی با خطرات و مشکلات امنیتی مرتبط با رایانه ، اینترنت و شنود ارتباطات اینترنتی
2. راههای نگاهبانی از اطلاعات خصوصی
3. روشهای عبور از فیلترینگ برای دسترسی به وب سایت های مسدود شده

برای دریافت جدیدترین نسخه این راهنما به اینجا مراجعه کنید: http://bit.ly/iran-computer-security

**توجه:  این راهنمای کوتاه تنها با هدف فراهم نمودن اطلاعات اولیه جهت عبور از فیلترینگ و برقراری ارتباط امن و بدون شنود تهیه شده است.هریک از روشهای ارائه شده دارای نقاط قوت و ضعف بوده و نباید استفاده از آنها احساس امنیت کاذب ایجاد کند. پس از عبور از فیلترینگ  لازم است جهت کسب اطلاعات تکمیلی درباره محدودیتها وخطرات هر روش به لینکهای ارائه شده مراجعه نمایید. این راهنمایی کاملا فنی است. تهیه کنندگان آن به هیچ گروه و دسته ای وابستگی ندارند.**

## آشنایی با خطرات و مشکلات امنیتی و شنود اینترنتی

خطرات ایمنی زیر واقعی بوده و احتمال رخ دادن آنها ممکن است بیشتر از آنچه که اکثر کاربران انتظار دارند باشد.

- دزدی اطلاعات شخصی و مالی شما
- شنود ارتباطات اینترنتی
- از بین رفتن اطلاعات بوسیله ویروس های رایانه ای
- ضبط و تفتیش رایانه شما
- دزیده شدن هویت الکترونیکی شما بوسیله شخص ثالث (Identity Theft)

## اقدامات ایمنی اولیه

### امنیت ایمیل

**توجه: ایمیل در حالت معمولی کاملا قابل شنود و دیدن بوسیله اشخاص روی خط (مثلا ISP شما) می باشد.**
برای کم کردن احتمال دسترسی به ایمیل وبی Web Mail توسط ISP ها از HTTPS استفاده کنید. بدین ترتیب دیدن ایمیل های موجود در صندوق پستی روی وب برای شما کم خطر می شود.

- توجه: ایمیل مجانی Yahoo امن نمی باشد و تا جایی که می دانیم ،امکان استفاده از HTTPS (بجز صفحه ورودی username/password) فراهم نیست.
- برای ایمیل گوگل gmail میتوانید به قسمت Settings و گزینه Always use https را انتخاب کنید. سپس دکمه Save Changes را برای ذخیره این تغییر فشار دهید. بهتر است از بایگانی پیغام های Chat را جلو گیری کنید. Settings بعد Chat بعد Never save chat history همچنین Only allow people that I've explicitly approved to chat with me and see when I'm online سپس Save Changes. دقت نمائید که در حالت عادی Chat در داخل صفحه فعال است. با انتخاب فلش در کناره Set Status Here (سمت چپ صفحه) سپس Sign out of chat آنرا غیر فعال کنید.

برای توضیحات بیشتر فصل پیشرفته این راهنما را بخوانید.

### توصیه های ایمنی

- نصب نرم افزار ضد ویروس. Symantec یا Norton یا AVG که مجانی است توصیه می شود: http://free.avg.com
- نصب نرم افزار پاکسازی: بسیاری از اسناد ، فایل ها و وب سایت هایی که از آنها استفاده می کنید حتی پس از پاک کردن بر روی کامپیوتر شما قابل دسترسی می باشند. اکیدا توصیه می کنیم که نرم افزار CCleaner را نصب و هر روز اجرا نمایید. وب سایت http://www.ccleaner.com را ببینید.
- باز نکردن ضمیمه های ایمیل
- انتخاب کلمه رمز (password) مناسب: از کلماتی که به راحتی قابل حدس زدن هستند استفاده نکنید. مثلا: سبز green ، ندا neda ، اسم خود یا خانواده. استفاده از ترکیب اعداد و علامات و حروف بزرگ و کوچک کلمه رمز را امن و غیر قابل حدس می کند.
- کلک ماهی گیری (Phishing): گاهی پیوندی (Link) در ایمیل برای شما فرستاده می شود با متنی است که به اسم یک وب سایت معروف است ولی در واقع با کلیک کردن روی آن شما به صفحه ای می روید که شبیه آن وب سایت است و اطلاعات شما را دریافت کرده و می دزدد. همیشه به آدرس نشان داده شده در بالای صفحه برازر دقت کنید و صرفا بعد از اطمینان از صحت آن اطلاعات کاربری و رمز خود را تایپ کنید. تصب Google Toolbar یا Yahoo Toolbar گاهی با دادن پیغام های خطر به شما کمک می کنند.
- مواظب آدرسهای وب سایت مشابه ای که برای فریب ایجاد شده اند باشید.

## عبور از فیلترینگ سایت های اینترنتی

بسیاری از راه حل های ارائه شده بصورت نرم افزار بدون احتیاج به نصب Installation هستند. در نتیجه شما می توانید نرم افزار را بر روی یک فلش درایو USB با خود حمل و در کافی نت ها نیز استفاده کنید.

## UltraSurf

UltraSurf که از محصولات شرکت UltraReach Internet Corp می باشد از نوعی ابزار پراکسی است که به منظور یاری رساندن به کاربران چینی طراحی شد تا به آنها در جستجوی آزادانه در اینترنت و دور از چشم سانسورچی های دولتی کمک کند.

برای دریافت نرم افزار به آدرس های: http://www.ultrareach.com/, http://www.ultrareach.net یا http://www.wujie.net مراجعه کنید. وبسایت آخر به زبان چینی است اما یافتن لینک بارگزاری در آن کار مشکلی نیست چراکه به زبان انگلیسی بر روی آن درج شده است.
پس از آنکه فایل "u.zip" را از یکی از آدرس های فوق بارگزاری نمودید، بر روی نمایه آن واقع در desktop رایانه خود کلیک راست کرده و بر روی " ... Extract here" کلیک کنید. در پایان، بر روی نمایه تازه ایجاد شده "u" دوبار کلیک کنید تا برنامه UltraSurf به اجراء درآید.

UltraSurf بصورت خودکار مرورگر Internet Explorer را اجراء کرده و صفحه جستجوی UltraSurf را به نمایش در می آورد: http://ultra1/ultrasurf.htm. همانطور که ملاحظه می کنید URL مندرج در این آدرس شکلی خاص دارد (فاقد نام دامنه مانند com. یا net. می باشد) و فقط در شبکه UltraSurf کار می کند. چنانچه صفحه مزبور نمایان شد، می توانید مطمئن باشید که از UltraSurf بطور صحیح و از طریق گذرگاه رمزگزاری شده SSL استفاده می کنید. اکنون با کمک مرورگر IE که قبلا توسط برنامه UltraSurf به اجرا در آمده می توان به جستجو در اینترنت پرداخت.

چنانچه مایل باشید برنامه کاربردی دیگری (مانند Firefix یا پیام رسان آنی Pidgin) را همراه با UltraSurf به کار ببرید، می باید آن را با استفاده از UltraSurf به عنوان یک سرور پراکسی تنظیم کنید. آدرس IP مربوطه عبارتست از: 127.0.0.1 و شماره درگاه آن 9666 می باشد.

### وب پراکسی

وب پراکسي به وب سایتی گفته می شود که اجازه مي‌دهد که يك سايت ديگر را از طريق آن ببينيد حتی وقتي که دسترسي مستقيم به آن سايت از جايي که شما هستيد مسدود شده باشد. يك وب پراکسي فرمي را نمايش مي‌دهد که در آن آدرس سايتي را که مي‌خواهيد مشاهده کنيد وارد مي‌کنيد.

وقتي از يك پراکسي وب استفاده مي‌کنيد، مجبور به نصب نرم‌افزار يا تغيير تنظيمهاي روي کامپيوتر خود نيستيد. در نتيجه از هر کامپيوتري از جمله کامپيوترهاي کافه‌هاي اينترنتي قابل استفاده است.

اشکالات وب پراکسی :

- بسیاری از وب پراکسی ها تبلیغات نامناسب دارند.
- عدم امنیت اطلاعات شما است. توصیه می شود برای دسترسی به اطلاعات مهم از وب پراکسی استفاده نشود.

مشکل دیگر وب پراکسی مسدود شدن بسیاری از آنها به مرور زمان است. شما می توانید آدرس های جدید را از طریق ایمیل یا گپ Instant Messenger یا وب سایت های مانند: http://iranproxyforum.com یا http://iranproxylist.com دریافت کنید.

## شبکه خصوصی مجازی (VPN; Virtual Private Network)

VPN یک ارتباط مجازی (تونل) بین کامپیوتر شما و یک سرور در نقطه‌ای دیگر از دنیا برقرار می‌کند به نحوی که کلیه بسته‌هایی(packets) که ارسال یا دریافت میکنید از طریق این تونل منتقل می‌شوند. درصورتی‌که این تونل امن باشد کلیه بسته‌های ارسالی روی آن رمزنگاری(encrypted) شده و قابل شنود یا کنترل نخواهندبود.
به عنوان مثال Hotspot Shield یا HSS را به شما معرفی می کنیم. می‌توانید HSS را از https://www.sesawe.net دانلود کنید یا به آدرس زیر ایمیل بزنید: **hss-sesawe@anchorfree.com**
در قسمت موضوع (subject) ایمیل، یکی از کلمات: hss، sesawe، hotspot، یا shield را وارد نمایید (استفاده از حروف کوچک یا بزرگ اشکالی ندارد).

پاسخ سوالات معمول درباره Hotspot Shield (متاسفانه امکان دارد این وب سایت در آینده مسدود شود.)

## Tor

این نرم افزار از جهت حفاظت اطلاعات شخصی بسیار پیشرفته است. اشکال آن سرعت پایین برای بعضی کاربران و زیاد بودن حجم فایل ها است. از طرفی می توان آن را، بدون نیاز به نصب روي ديسک سخت کامپيوتر، در هر PC ويندوزي مورد استفاده قرار داد.

**Browser Bundle Tor**

مي‌توانيد Tor Browser Bundle را از سايت وب torproject.org دانلود کنيد، هم بصورت يك فايل واحد (25 مگابايت) يا يك نسخه "چند قسمتی" که شامل چند فايل 1.4 مگابايتي است. اگر اتصال اينترنت شما کند و غيرقابل اطمينان است، ممکن است دانلود کردن نسخه چند قسمتی راحت تر از يك فايل خيلي بزرگ باشد.
اگر سايت وب torproject.org در محلي که هستيد فيلتر مي‌شود، در موتور جستجوي مورد علاقه خود عبارت "tor mirrors" را تايپ کنيد: احتمالا نتايج جستجو حاوي آدرسهاي جايگزين براي دانلود Tor Browser Bundle خواهد بود.

**دریافت نرم افزار Tor:**

- از راه وب و بصورت يك فايل واحد: https://www.torproject.org/torbrowser
- اگر سرعت اینترنت شما پایین است فایلها را در چند قسمت دریافت کنید (https://www.torproject.org/torbrowser/split.html)
- اگر وب سایت های بالا مسدود شده اند می توانید از دوستان و آشنا ها درخواست کنید که فایل ها را برای شما ایمیل کنند. (https://www.torproject.org/torbrowser/split.html)

اگر بعد از دو يا سه بار تلاش هنوز مرورگر Tor کار نکرد، ممکن است Tor توسط ISP شما بلوکه شده باشد و بايد سعي کنيد از ويژگي پل Tor Bridge استفاده کنيد.

## نرم افزارهای دیگر

- Freegate: وی سایت http://www.dit-inc.us/freegate
- Your Freedom: وب سایت http://www.your-freedom.net
- GPass: وب سایت http://gpass1.com/gpass

## ترفندهاي ساده

چندين تکنيك براي رهايی از فيلترينگ اينترنت وجود دارد. اگر هدف شما رسيدن ساده به صفحه‌ها و خدماتي در اينترنت باشد که از محل شما بلوکه شده است و شما نگران نيستيد که آيا افراد مي‌توانند دور زدن شما را کشف و نظارت کنند، اين تکنيکها همه چيزي است که به آن نياز داريد:

- استفاده از سايتهاي وب واسط براي رسيدن به محتواي بلوکه شده
- بازيابي صفحه‌هاي وب بلوکه شده به کمك ايميل

#### استفاده از سايتهاي واسط

چند راه مختلف براي اينکه بتوانيد از سايتهاي وب واسط، به جاي دسترسي مستقيم، به محتواي مورد نظر راه پيدا کنيد، وجود دارد.

##### صفحه‌هاي ذخيره شده

بيشتر موتورهاي جستجو کپي‌هايي از صفحه‌هاي وبي را که پيشتر شاخص‌گذاري کرده‌اند نگهداري مي‌کنند که به آنها صفحه‌هاي ذخيره شده (cached) مي‌گويند. وقتي يك سايت وب را جستجو مي‌کنيد، به دنبال يك لينك کوچك با برچسب "cached" بعد از نتايج جستجو بگرديد. چون يك کپي از صفحه‌هاي بلوکه شده را از سرورهاي موتور جستجو بازيابي مي‌کنيد نه از خود سايت بلوکه شده، مي‌توانيد به محتواي بلوکه شده دسترسي داشته باشيد. ولي برخي کشورها سرويسهاي صفحه‌هاي ذخيره شده را نيز براي مسدود سازی هدف مي‌گيرند.

##### جمع‌کننده‌هاي RSS

جمع‌كننده‌هاي RSS سايتهاي وبي هستند كه به شما اجازه مي‌دهند در آنها عضو شويد و محتواي RSS را كه جريانهايي از خبرهاي و ساير اطلاعات است كه توسط سايتهايي كه انتخاب كرده‌ايد تغذيه مي‌شوند، بخوانيد. يك جمع‌كننده RSS به سايتهاي وب وصل مي‌شود و محتوايي را كه شما انتخاب كرده‌ايد دانلود مي‌كند و نمايش مي‌دهد. چون اين جمع‌كننده است كه به سايتهاي وب وصل مي‌شود و نه شما، ممكن است بتوانيد به سايتهايي كه بلوكه شده‌اند دسترسي داشته باشيد. البته اين تكنيك فقط درصورتي كار مي‌كند كه سايتهاي وب، محتواي خود را بصورت محتواي RSS منتشر كنند و بنابراين مفيدترين شيوه براي سايتهاي خبري و وبلاگهاست. تعداد زيادي جمع‌كننده RSS آنلاين مجاني موجود است. بعضي از عمومي‌ترين آنها (Google Reader http://reader.google.com) و (Bloglines http://www.bloglines.com) هستند.

#### مترجمها

سرويسهاي مترجم زبان زيادي دراينترنت وجود دارد كه اغلب توسط موتورهاي جستجو ارايه مي‌شوند. اگر از طريق يك سرويس ترجمه به يك سايت وب وصل شويد، اين سرويس ترجمه است كه به سايت بلوكه شده دسترسي پيدا مي‌كند نه شما. به اين ترتيب شما ميتوانيد محتواي بلوكه شده‌اي را كه به زبانهاي مختلفي ترجمه شده است، بخوانيد.

مي‌توانيد از سرويس ترجمه براي عبور از بلوكه شدن استفاده كنيد، حتا اگر واقعا نيازي به ترجمه متن نداشته باشيد. براي اينكار زباني را براي ترجمه انتخاب كنيد كه سايت وب اصلي به آن زبان نباشد تا سايت به زبان اصلي برگردانده شود. براي مثال براي استفاده از سرويس ترجمه براي مشاهده يك سايت وب انگليسي زبان، ترجمه از چيني به انگليسي را انتخاب كنيد. سرويس ترجمه فقط بخشهاي چيني را ترجمه مي‌كند (هيچ بخشي) و بخشهاي انگليسي را ترجمه نشده رها مي‌كند (كه همه صفحه وب است).

معروف ترين سرويسهای ترجمه عمومی http://babelfish.yahoo.com و
http://translate.google.com هستند.

#### فيلترهاي پهناي باند پايين

فيلترهاي پهناي باند پايين، سرويسهاي وبي هستند كه به منظور مرور ساده‌تر وب در جاهايي كه سرعت اتصال پايين است، طراحي شده‌اند. آنها تصاوير را حذف مي‌كنند يا كاهش مي‌دهند، تبليغات را حذف مي‌كنند و سايت وب را براي كم كردن داده‌ها فشرده مي‌كنند، بنابراين دانلود آن سريعتر است. اما مانند سرويسهاي ترجمه و جمع‌آوري، مي‌توانيد با بازيابي سايتهاي وب از سرورهاي فيلترهاي پهناي باند پايين، به جاي كامپيوتر خود، براي عبور از سايتهاي وب بلوكه شده استفاده كنيد. http://loband.org يك فيلتر پهناي باند پايين است.

#### استفاده از سرويسهاي ايميل

سرويسهاي ايميل و وب‌ميل مي‌توانند براي اشتراك‌گذاري مستندات با گروهي از دوستان يا همكاران يا حتا مرور وب بكار روند.

#### دسترسي به صفحه‌هاي وب به كمك ايميل

همچون فيلترهاي پهناي باند پايين، سرويسهايي با هدف افراد داراي اتصالهاي اينترنت كند يا نامطمين وجود دارد كه به شما اجازه درخواست يك صفحه وب از طريق ايميل را مي‌دهد. اين سرويس يك ايميل پاسخ مي‌فرستد كه حاوي صفحه وب مورد تقاضا يا در بدنه پيام يا به عنوان پيوست نامه است. كاربرد اين سرويسها مي‌تواند كاملا پرزحمت و طاقت‌فرسا باشد، چون لازم است براي يك يا چند صفحه وب درخواستهاي جداگانه بفرستيد و سپس منتظر پاسخ بمانيد، اما در موقعيتهاي خاص مي‌توانند براي رسيدن به صفحه‌هاي وب بلوكه شده بسيار موثر باشند، به ويژه اگر آنها را از يك سرويس وب‌ميل امن بكار گيريد.

يك نمونه از اين سرويس pagegetter.com است. براي استفاده از آن، يك ايميل حاوي يك يا بيشتر URL در

موضوع يا بدنه پيام به web@pagegetter.com بفرستيد. سپس بصورت خودكار صفحه‌هاي وب درخواستي را بطور كامل و به همراه بخشهاي گرافيكي دريافت خواهيد نمود. صفحه‌هاي وب داراي فريم در چند ايميل ارسال خواهند شد، چون بيشتر نرم‌افزارهاي كلاينت ايميل نمي‌توانند فريمها را نمايش دهند. (فريمها راهي براي نمايش چند صفحه در يك صفحه نمايش است.) اما اگر نرم‌افزار كلاينت ايميل، فريمها را پشتيباني كند ( براي مثال Outlook Express) مي‌توانيد همه فريمها را در يك پيام دريافت كنيد. در اين حالت، ايميل را به frames@pagegetter.com بفرستيد.

براي دريافت يك نسخه فقط-متني از صفحه درخواستي، از text@pagegetter.com استفاده كنيد. اين حالت به خصوص براي PDAها، تلفنهاي همراه و سيستمهاي ايميل فقط-متني مفيد است. همينطور مي‌توانيد براي بازيابي يك صفحه كامل HTML بدون بخشهاي گرافيكي يك ايميل به HTML@pagegetter.com بفرستيد.

سرويس مشابهي در web2mail.com پيدا مي‌شود. براي استفاده از آن، يك پيام حاوي آدرس وب (URL) صفحه درخواستي در خط موضوع آن به www@web2mail.com ارسال كنيد. همچنين مي‌توانيد با تايپ عبارتهاي جستجو در خط موضوع، جستجوهاي ساده وب را انجام دهيد. براي مثال مي‌توانيد براي جستجوي ابزارهاي دور زدن سانسور عبارت "search censorship circumvention tools" را در موضوع يك پيام ايميل وارد كنيد و آن را به www@web2mail.com بفرستيد.

مي‌توانيد اطلاعات و پشتيباني بيشتري در اين موضوع درليست پستي ACCMAIL پيدا كنيد. براي ثبت نام، يك ايميل حاوي "SUBSCRIBE ACCMAIL" در بدنه آن به listserv@listserv.aol.com بفرستيد.

**استفاده از وب‌ميل براي به اشتراك‌گذاردن مستندات**

اگر تلاش مي‌كنيد مستنداتي را بصورت آنلاين به اشتراك بگذاريد ولي مي‌خواهيد كساني كه آنها را مي‌بينند كنترل كنيد، مي‌توانيد آنها را در يك فضاي خصوصي نگهداري كنيد كه فقط براي كساني قابل مشاهده است كه داراي كلمه رمز درست هستند. يك راه ساده براي به اشتراك‌گذاري مستندات با يك گروه كوچك از دوستان يا همكاران، استفاده از يك حساب پستي در يك ارايه كننده ايميل آنلاين مانند(Gmail
(https://mail.google.com است و به اشتراك گذاردن نام كاربر و كلمه رمز با كساني كه لازم است به مستندات دسترسي داشته باشند. حتما در تنظيمات gmail از Always use https استفاده كنيد. چون بيشتر ارايه كنندگان وب‌ميل مجاني هستند، به آساني مي‌توان در فواصل زماني از حساب تازه‌اي استفاده كرد تا كار را براي كسي كه در گروه نيست و پي‌گير آن است كه شما چكار مي‌كنيد، مشكلتر كنيد. ليستي از ارايه‌كنندگان ايميل آنلاين مجاني در http://www.emailaddresses.com/email_web.htm موجود است.

مزايا و ريسكها استفاده از اين تكنيكها سريع و آسان است؛ مي‌توانيد با كمترين تلاش آنها را تجربه كنيد. بسياري از آنها حداقل در بيشتر اوقات كار خواهند كرد. ولي اشكال كار در اينجاست كه تكنيكهاى مزبور اغلب به راحتي كشف و بلوكه مي‌شوند. همينطور چون محتوا را رمزگذاري و ارتباطهاي شما را مخفي نمي‌كنند، مورد هدف نظارت و مسدود سازى بر اساس كلمه-كليدي هستند.

## ايجاد محيط امن در رايانه شخصى

اطلاعات خصوصى موجود بر روى رايانه شما همواره در معرض خطرات مختلف است. رايانه شم ممكن است ضبط يا دزديده شود. گاهى رايانه در اختيار شما است ولى مبتلا به ابزارهاى مختلف دزدى اطلاعات (Spayware) مى باشد. راه هاى زير تا حدودى به شما كمك مى كند.

**به رمز كردن فايل ها**

فایل ها و اسناد مهم خود را همواره بصورت رمز شده بر روی رایانه شخصی خود نگهدارید یا ارسال کنید. در دسترس ترین نرم افزارها WinZip و WinRar هستند. WinRar مجانی را می توانید از http://www.rarlab.com/download.htm دریافت کنید.

### نصب نرم افزار پاکسازی

بسیاری از اسناد ، فایل ها و وب سایت هایی که از آنها استفاده می کنید حتی پس از پاک کردن بر روی کامپیوتر شما قابل دسترسی می باشند. اکیدا توصیه می کنیم که نرم افزار CClean را نصب و هر روز اجرا نمایید. وب سایت http://www.ccleaner.com را ببینید.

این محل حتی بعد از استفاده از CCleaner نیاز به پاک سازی دارد: C:\Documents and Settings\your_username\Local Settings\Temp

### پاک کردن کامل فایل ها

مطلب بسیار مهمی که بسیاری از کاربران رایانه از آن مطلع نیستند باقی ماندن اطلاعات فایل ها حتی بعد از پاک کردن معمولی Delete است. در اکثر محیط های رایانه ای پاک کردن معمولی یک فایل به معنای از بین بردن اسم فایل در فهرست فایل ها است. اطلاعات و داده های اصلی همچنان بر روی دیسک سخت یا حافظه های دیگر باقی می مانند. برای پاک کردن واقعی فایل ها از نرم افزارهای مخصوص مانند Eraser در http://eraser.heidi.ie استفاده کنید.

اگر به پاک کردن کل دیسک سخت نیاز دارید می توانید از نرم افزارهای زیر استفاده کنید. احتیاط کنید! توجه نمایید که تمام اطلاعات شما از بین می رود. دقت کنید که برق و باطری رایانه باید برای چند ساعت بطور متمادی وصل باشد در غیر این صورت دیسک سخت در نیمه کار قفل شده و مشکل سخت افزاری ایجاد می شود.
http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml و http://www.dban.org

### به رمز کردن دیسک سخت

می توانید کل دیسک سخت (Hard Drive) را به رمز کنید. به عنوان نمونه می توانید از نرم افزارهای زیر استفاده کنید:

- http://disk-encryption.comodo.com
- http://www.truecrypt.org
- http://www.scherrer.cc/crypt

## ارتباط اینترنتی به صورت ناشناس (جلوگیری از شنود)

بسیاری از ابزارهای فیلتر شکنی که در بالا به آنها اشاره شد با ناشناس بودن شما حداقل در قسمتی از مسیر ارتباط اینترنتی کمک می کنند. ولی اکثر آنها محدودیت های عمده ای در را به رمز سازی از شروع تا پایان دارند. ابزارهای زیر کمک می کنند که ارتباطات از ابتدای ایجاد بر روی رایانه شما به رمز بشوند.

### ایمیل رمز شده

- 
- PGP: این شناخته معروف ترین و بهترین روش های به رمز کردن ایمیل است. شما می توانید آنرا بر روی Outlook یا Thunderbird به صورت Plugin نصب کنید.راحت ترین روش استفاده از آن نصب نرم افزار FireGPG http://getfiregpg.org برای وب ایمیل های gmail و Yahoo بر روی مرورگر Firefox است. برای استفاده از روش های دیگر به این راهنما مراجعه کنید:
  http://www.encryptedemail.org
- Hushmail: برای باز کردن یک حساب ایمیل رمز شونده و مجانی به http://hushmail.com بروید. استفاده از این ایمیل ساده است و دریافت کننده می تواند حتی با جواب به یک سوال از قبل تعیین شده ایمیل را بخواند. مشکل کوچک این سیستم نگهداری کلید خصوصی بر روی سرور است.

### صحبت کردن (تلفن اینترنتی) محرمانه Private Voice Over IP

این مطلب که تلفن اینترنتی قابل شنود است یا نه موضوعی روشن نیست. توصیه می شود از تلفن اینترنتی محرمانه زیر استفاده کنید.

- zphone: یک نرم افزار رمز کردن صدا است که بر روی Google Talk, Yahoo Voice و غیره نصب می شود. اینجا را ببینید: http://zfoneproject.com/getstarted.html
- Skype: یک نرم افزار معروف تلفن اینترنتی است که ممکن است امن باشد ( صدا و Instant Messaging) .لیکن گزارش هایی در مورد قابل شنود بودن Skype وجود دارد.

در صورتی که از روش های VPN استفاده می کنید تمام ترافیک اینترنت شما خصوصی می شود. تلفن اینترنتی هم تا محلی که به آن با VPN وصل شده اید خصوصی است. چون این محل معمولا خارج از کشور است مساله شنود تا حدود مناسبی حتی بدون استفاده از روش های رمز کردن بالا حل می شود.

## گپ محرمانه Private Instant Messaging

بسیاری از سرویس های گپ Instant Messaging قابل شنود هستند. توصیه می شود از گپ محرمانه استفاده کنید.

- Skype ممکن است امن باشد ( صدا و Instant Messaging) . گزارش های در مورد قابل شنود بودن آن وجود دارد.
- گپ محرمانه Private Instant Messaging . این نرم افزار(Off-the-Record) مجانی است. راحت ترین روش تصب Pidgin سپس OTR plugin for Pidgin می باشد. Pidgin را به زبان انگلیسی نصب کنید ( کار با فارسی آن مشکل است).

در صورتی که از روش های VPN استفاده می کنید تمام ترافیک اینترنت شما خصوصی می شود. تلفن اینترنتی هم تا محلی که به آن با VPN وصل شده اید خصوصی است. چون این محل معمولا خارج از کشور است مساله شنود تا حدود مناسبی حتی بدون استفاده از روش های رمز کردن بالا حل می شود.

## فرستادن پیغام محرمانه ای که با زمان از بین می رود

گاهی یگ پیغام صرفا ارزش کوتاه مدت دارد و بهتر است بعد از مدتی پاک شود. ما این روش را پیغام کاراگاه Gadget می نامیم. شما می توانید یک آدرس کوتاه و حتی قابل به حافظه سپردن را اینجا ایجاد کنید:

https://sturly.com/meta-short-url.php

توجه کنید که https برای ایجاد پیغام و URL نهایی قابل استفاده است ولی در حال حاضر certificate برای سایت دیگری صادر شده است و ممکن است باعث بروز اخطار در مرورگر شود.هرچند این اخطار خیلی نگران کننده نیست ما دنبال پیدا کردن سرویس بهتری برای معرفی به شما هستیم.

## دریافت جدیدترین نسخه این راهنما

به اینجا مراجعه کنید: http://bit.ly/iran-computer-security

## کمک به گسترش این راهنما

اگر علاقه مند به کمک به گسترش این راهنما هستید مطالب خود را به ما ایمیل کنید:
iran.computer.security@gmail.com
هرگونه اشکال و نقص را حتماً به ما یادآوری کنید.

## منابع

برای اطلاعات بیشتر به منابع زیر مراجعه کنید. از این منابع در تهیه این راهنما استفاده شده است.

1. کمیته مبارزه با سانسور در ایران: http://iranproxyforum.com و http://www.cac-iran.com

2. SESAWE: http://sesawe.net/spip.php?lang=fa
3. Global Internet Freedom Consortium: http://www.internetfreedom.org
4. Security in-a-box در http://security.ngoinabox.org
5. راهنمای گزارشگران بدون مرز: http://www.rsf-persan.org/article16200.html
6. راهنمای عبور از سانسور اینترنتی برای همگان: http://civisec.org/guides/everyones-guides