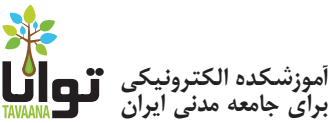
امنیت دیجیتال پیشرفته

آموزشکده الکترونیکی
برای جامعه مدنی ایران

پروژهٔ

e-collaborative
for civic education



http://www.tavaana.org

پروژهٔ

e-collaborative
for civic education

http://www.eciviced.org

امنیت دیجیتال پیشرفته

ناشر: E-Collaborative for Civic Education

تدوین: نیما راشدان

e-collaborative
for civic education

E-Collaborative for Civic Education (ECCE) یک سازمان غیرانتفاعی در ایالات متحده آمریکا، تحت 501c3 است که از فن‌آوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیانگذاران و مدیران این سازمان، اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از یک جامعهٔ سیاسی دموکراتیک پایه و اساس کار است؛ همان طور که حقوق عام بشر که هر شهروندی باید از آنها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک تک شهروندان و امنیت برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند، است.

ما پروژهٔ اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعهٔ مدنی ایران» را در سال ۲۰۱۰ تأسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس ماندن دانشجویان، به یک جامعهٔ آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وبلاگ‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زندهٔ دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با فعالان و روشنفکران، دستورالعمل‌های خودآموزی، کتابخانهٔ مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاورهٔ آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعهٔ توانایی‌های آموزشکده توانا متوجه گرد آوردن بهترین متفکران ایرانی و صداهای محذوف است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان توسط جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فن‌آوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هموطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما

اکبر عطری — مریم معمارصادقی

فهرست مطالب

مقدمه نویسنده

این جزوه برای کمک به دانشجویان درس «امنیت دیجیتال پیشرفته» آموزشکده توانا تهیه شده است. پیش از هر چیز توجه به این نکته لازم است که هیچ جزوه‌ای نمی‌تواند در بر گیرنده همه مواد مورد نیاز برای ارتقای امنیت دیجیتال کاربران باشد؛ گستردگی مباحث و تهدیدات دنیای دیجیتال، باعث شده است که هر کاربر بر اساس نیاز و شرایط خاص محیط پیرامونی خود، نیازمند تدابیر جداگانه‌ای برای حفظ هویت شخصی، امنیت داده‌ها و ارتباطات خود باشد.

هدف اصلی این جزوه بارورکردن توان دانشجویان با میزان آگاهی دیجیتال متوسط و پیشرفته برای کمک کردن به کاربران ابتدایی است. با ذکر مثال‌ها و آمار متعددی تلاش شده است تا روش‌های آموزشی مؤثر و کارآمدی به شرکت‌کنندگان دورهٔ امنیت دیجیتال پیشرفته منتقل شود.

تأکید ما در سراسر دوره بر انتقال مفاهیم بوده است و نه فهرستی از همه تهدیدها و راهکارهای مقابله با آنها. چنین فهرستی اولا بسیار متغیر خواهد بود و دائما نیازمند به روز رسانی است و ثانیا به دلیل محدودیت حجمی، جزوه هرگز نمی‌تواند در بر گیرنده حتی بخش کوچکی از تهدیدهای دنیای دیجیتال باشد. از این رو تلاش شده است تهدیدها و راه‌های پیشگیری و مقابله با آنها، در قالب مفاهیم به دانشجویان منتقل شود.

هدف دیگر این دوره تربیت آموزش‌دهندگان فنون امنیت دیجیتال است. در کادرهای داخل متن که راهنمای آموزش‌دهندگان است، نکات ویژه کاربرانی که علاقه‌مند به آموزش دادن فنون امنیت دیجیتال

هستند، آمده است.

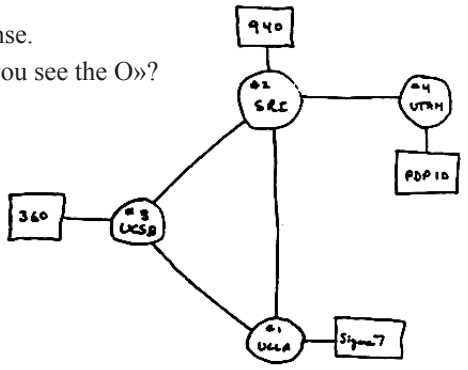
کارآمدترین شیوهٔ استفاده از این جزوه، مطالعهٔ آن هم‌زمان با مشاهدهٔ ویدئوهای آموزشی توانا در آدرس زیر و همچنین فروم‌های تواناتِک و حضور در مباحث آنلاین امنیت دیجیتال توانا است:

http://www.youtube.com/user/tavaana2010

۱
تهدیدها در دنیای دیجیتال

بسیاری نقطه تولد اینترنت را در لحظه اتصال چند کامپیوتر توسط شبکه آزمایشی ARPANET می‌دانند. در حقیقت نخستین مبادله «پاکت‌های داده»[۱] تحت پروتکلی موسوم به «۱۸۲۲»[۲] با اتصال کامپیوترهای شبکه ARPA به یکدیگر انجامید. ساعت ۲۲:۳۰ دقیقه ۲۹ اکتبر ۱۹۶۹ دو حرف L و O از طریق نخستین اتصال ARPANET میان دانشگاه کالیفرنیا – لس‌آنجلس (UCLA) و موسسه تحقیقاتی استنفورد مبادله شدند:

«Do you see the L»?
«Yes, we see the L», came the response.
We typed the O, and we asked «Do you see the O»?
«Yes, we see the O»



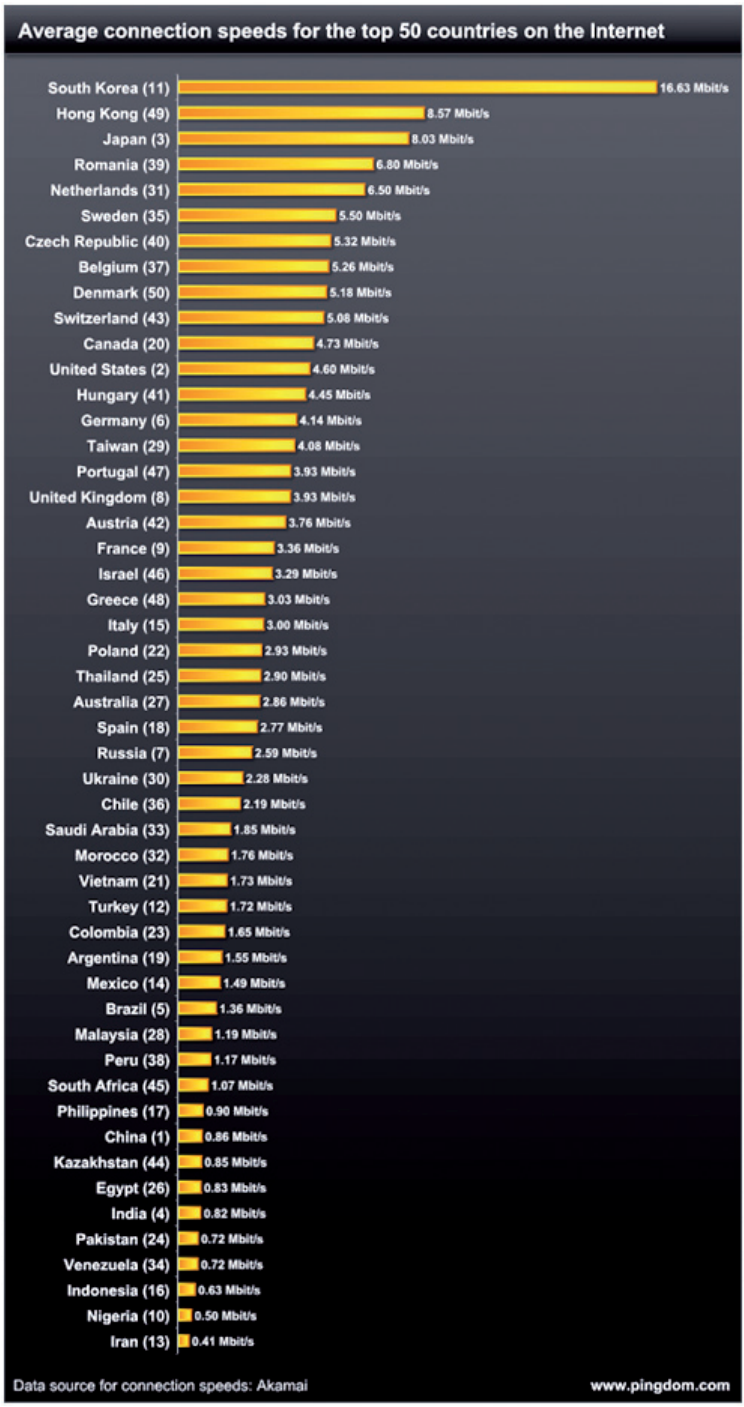
THE ARPA NETWORK
DEC 1969
4 NODES

ابعاد اینترنت

رشد انفجاری اینترنت و وب جهانی در ربع قرن گذشته و افزایش حیرت‌انگیز نفوذ و تأثیر آن در همه جنبه‌های زندگی، رویکردی بی‌سابقه در تاریخ تمدن بشری است.

برای ارائه تصویری متناسب از ابعاد اینترنت می‌توان از مقایسه‌های آماری نظیر موارد ذیل استفاده کرد:

- دو میلیارد نفر به شبکه اینترنت دسترسی دارند؛ تا سال ۲۰۲۰ این تعداد دو برابر خواهد شد.
- دو ماه آپلود ویدئو بر روی یوتیوب برابر با مجموع تولید ۲۴ ساعته غیرتکراری شبکه‌هایی نظیر NBC، ABC و CBS در طول ۶۸ سال است.
- جذب ۵۰ میلیون مخاطب برای اینترنت ۵ سال طول کشید، این عدد برای تلویزیون ۱۳ سال و برای رادیو ۳۸ سال بوده است.
- روزانه ۲۱۰ بیلیون ایمیل ارسال می‌شود. ۸۰ درصد این تعداد هرزنامه یا Spam است.
- سه میلیون عکس روزانه روی سایت Flickr آپلود می‌شود.
- روزانه دو میلیارد ویدئو روی یوتیوب مشاهده می‌شود، محبوب‌ترین ویدئوها به ترتیب: جاستین بیبر، لیدی گاگا و «چارلی انگشت منو گاز گرفت» هستند.
- روزانه ۵۰ میلیون توییت فرستاده می‌شود. توییتر بیش از ۲۵۰ میلیون کاربر دارد.
- از ۴۸ آگهی مرتبط با پول درآوردن در خانه، ۴۷ آگهی کلاه‌برداری است.
- از هر ۸ شهروند کشورهای پیشرفته، یک نفر علایم اعتیاد به اینترنت را نشان می‌دهد. اعتیاد به اینترنت یعنی مجموعه رفتارهایی که نشان می‌دهد کاربر توان کنترل و مدیریت زمان را در برابر اینترنت و تجهیزات آنلاین‌شونده از دست می‌دهد.
- در سال ۲۰۰۶ یاهو برای خرید فیس‌بوک، یک میلیارد دلار پیشنهاد کرد. ارزش کنونی فیس‌بوک بیش از ۹۵ بیلیون دلار تخمین زده می‌شود.
- فیس‌بوک بیش از یک میلیارد نفر عضو دارد. (سپتامبر ۲۰۱۲)
- شبکه‌های مجازی، ۱۸ درصد از زمان آنلاین بودن کاربران را به خود اختصاص داده‌اند؛ مدت زمانی که از سال ۲۰۰۶ تا ۲۰۱۱ تقریبا سه برابر شده است.
- هر کاربر فیس‌بوک به طور متوسط ۲۳ دقیقه از وقت روزانه خود را در فیس‌بوک می‌گذراند.
- بسیاری از صاحب‌نظران میزان سرعت متوسط اینترنت در هر کشور را در نسبت مستقیم با ظرفیت آن کشور برای رشد اقتصادی و علمی ارزیابی می‌کنند. نمودار صفحه بعد، وضعیت اسف‌بار اینترنت در ایران را به نمایش می‌گذارد.


Average connection speeds for the top 50 countries on the Internet
South Korea (11) 16.63 Mbit/s
Hong Kong (49) 8.57 Mbit/s
Japan (3) 8.03 Mbit/s
Romania (39) 6.80 Mbit/s
Netherlands (31) 6.50 Mbit/s
Sweden (35) 5.50 Mbit/s
Czech Republic (40) 5.32 Mbit/s
Belgium (37) 5.26 Mbit/s
Denmark (50) 5.18 Mbit/s
Switzerland (43) 5.08 Mbit/s
Canada (20) 4.73 Mbit/s
United States (2) 4.60 Mbit/s
Hungary (41) 4.45 Mbit/s
Germany (6) 4.14 Mbit/s
Taiwan (29) 4.08 Mbit/s
Portugal (47) 3.93 Mbit/s
United Kingdom (8) 3.93 Mbit/s
Austria (42) 3.76 Mbit/s
France (9) 3.36 Mbit/s
Israel (46) 3.29 Mbit/s
Greece (48) 3.03 Mbit/s
Italy (15) 3.00 Mbit/s
Poland (22) 2.93 Mbit/s
Thailand (25) 2.90 Mbit/s
Australia (27) 2.86 Mbit/s
Spain (18) 2.77 Mbit/s
Russia (7) 2.59 Mbit/s
Ukraine (30) 2.28 Mbit/s
Chile (36) 2.19 Mbit/s
Saudi Arabia (33) 1.85 Mbit/s
Morocco (32) 1.76 Mbit/s
Vietnam (21) 1.73 Mbit/s
Turkey (12) 1.72 Mbit/s
Colombia (23) 1.65 Mbit/s
Argentina (19) 1.55 Mbit/s
Mexico (14) 1.49 Mbit/s
Brazil (5) 1.36 Mbit/s
Malaysia (28) 1.19 Mbit/s
Peru (38) 1.17 Mbit/s
South Africa (45) 1.07 Mbit/s
Philippines (17) 0.90 Mbit/s
China (1) 0.86 Mbit/s
Kazakhstan (44) 0.85 Mbit/s
Egypt (26) 0.83 Mbit/s
India (4) 0.82 Mbit/s
Pakistan (24) 0.72 Mbit/s
Venezuela (34) 0.72 Mbit/s
Indonesia (16) 0.63 Mbit/s
Nigeria (10) 0.50 Mbit/s
Iran (13) 0.41 Mbit/s
Data source for connection speeds: Akamai
www.pingdom.com

تهدیدهای دیجیتالی ظاهر می‌شوند

در فاصله زمانی کوتاهی پس از تولد و رواج شبکه‌های کامپیوتری با قابلیت برقراری ارتباطات از راه دور، تهدیدهای دیجیتالی نیز ظاهر شدند. یکی از نخستین مثال‌های تهدید تکنولوژیک سوء استفاده یک تکنسین الکترونیک از خطوط تلفن راه دور، با استفاده از سوت اسباب بازی در قوطی‌های سرل Cap'n Crunch بود. او سوت را به شکلی دست‌کاری کرد که می‌توانست با نواختن در فرکانس ۲۶۰۰ هرتز، وارد سیستم ارتباط راه دور شرکت مخابراتی AT&T شود.[۳] از آن تاریخ ده‌ها هزار تهدید خرد و کلان اینترنتی، امنیت داده‌های دیجیتال را تهدید کرده‌اند.

ماجرای Kevin Mitnick می‌تواند به روشنی برای ارائه تصویری قابل فهم از یک «هکر» (نفوذگر به شبکه‌های کامپیوتری) در سال‌های آغازین انقلاب دیجیتال مورد استفاده قرار گیرد:

۱. کوین در سن ۱۲ سالگی با استفاده از روش‌های «مهندسی اجتماعی» و با فریب یک راننده اتوبوس، از او محل تهیه دستگاه‌های سوراخ کن بلیط در اتوبوس‌های لس‌آنجلس را یاد گرفت و پس از آن دیگر بلیط نخرید. او در نوجوانی آموخت: بهترین راه برای به دست آوردن پسورد، شماره کاربری و... نه توانایی‌های خارق‌العاده فنی، بلکه «مهندسی اجتماعی» و «فریب انسان‌ها» است.

۲. در ۱۶ سالگی باز با روش‌های «مهندسی اجتماعی» شماره تلفن دسترسی به سیستم کامپیوتری شرکت DEC را به دست آورده و نرم‌افزار تولیدی این شرکت را برای خود کپی کرد.

۳. کوین میتنیک بعدها Fujitsu، Sun Microsystems، Nokia، NEC، Motorola Siemens و IBM را هم هک کرد.[۴]

مورد دوم برای تجسم ابعاد عظیم عملیات سایبری داستان Gary McKinnon است؛ فردی که تصور می‌کرد دولت آمریکا و نهادهای نظامی – اطلاعاتی این کشور «شواهد وجود بشقاب‌پرنده‌ها» را مخفی کرده‌اند. او ۹۷ سایت بسیار حساس نظامی ایالات متحده آمریکا و همچنین سایت ناسا را در طی مدتی ۱۳ ماهه از فوریه ۲۰۰۱ تا مارس ۲۰۰۲ تحت شناسه «Solo» هک کرد. از جمله این سایت‌ها می‌توان به سایت نیروی هوایی ایالات متحده، وزارت دفاع (پنتاگون)، نیروی دریایی و ناسا (سازمان تحقیقات فضایی ایالات متحده آمریکا) اشاره کرد. دعوای حقوقی بر سر انتقال گری مک‌کینون اسکاتلندی به ایالات متحده و محاکمه او سال‌هاست که ادامه دارد.

طبقه‌بندی تهدیدهای دیجیتالی برای دانشجویان

تهدیدهای دیجیتالی را می‌توان به اشکال مختلفی طبقه‌بندی کرد:

انواع مختلف تهدیدها حسب جنس تهدید

نوع تهدید	انگیزه تهدید	هدف تهدید	نحوه تخریب
جنگ سایبری	نبرد با رقیب سیاسی یا امنیتی	تاسیسات زیربنایی، نیروگاه‌های برق، مراکز نظامی	تخریب و اخلال در تاسیسات و زیرساخت‌های حیاتی
جاسوسی سایبری	کسب اطلاعات نظامی، صنعتی، تجاری	دولت‌ها، ارتش‌ها، بنگاه‌های اقتصادی و علمی و احزاب سیاسی	سرقت اطلاعات
تروریسم سایبری	تهدید شهروندان، دشمنان و یا جذب نیرو برای اهداف تروریستی	شهروندان، جوانان و نوجوانان	استخدام افراد تازه کار به منظور آموزش ترور
جرم سایبری	اقتصادی، مالی، سودجویی	شهروندان و بنگاه‌های اقتصادی	سرقت اطلاعات بانکی، کارت‌های اعتباری و...
تخریب	دشمنی شخصی	شهروندان	حمله، تخریب شخصیت
هکتیویسم	اهداف ایدئولوژیک و سیاسی، کنشگری اجتماعی با تسلط به تکنولوژی‌های دیجیتال	بنگاه‌های اقتصادی، دولت‌ها، احزاب سیاسی یا گروه‌های اجتماعی و مدنی	حمله، از کار انداختن سایت‌های اینترنتی، نفوذ با هدف کسب اطلاعات محرمانه

برای توضیح موارد فوق می‌توان از مثال‌هایی شبیه موارد زیر استفاده کرد:[۵]

نوع تهدید	مثال
جنگ سایبری	ویروس استاکس نت (بمباران الکترونیک تأسیسات هسته‌ای ایران)، حمله هکرهای مورد حمایت دولت روسیه به استونی
جاسوسی سایبری	شبکه ارواح یا گوست نت، جعل گواهینامه‌های امنیتی توسط ایران
تروریسم سایبری	فعالیت‌های سایبری شبکه القاعده، جندالله، حزب‌الله و حماس
جرم سایبری	کلاه‌برداری اینترنتی، حقه‌های موسوم به بانک‌های سوئیس، لاتاری‌های جعلی

تخریب	cyber bullying، حملات شخصی علیه نوجوانان در مدارس و کالج‌ها
هکتیویسم	حملات گروه «انانیمس»، حمله معترضان ایرانی به وب‌سایت‌های فارس‌نیوز و رجانیوز در سال ۱۳۸۸

تقسیم‌بندی تهدید بر اساس انتخاب قربانی

قربانی ناشناس و تصادفی

در این نوع حملات، قربانی به صورت اتفاقی به دام هکرها می‌افتد. اساسا برای حمله‌کننده یا نفوذگر اهمیتی ندارد که قربانی چه مشخصاتی دارد، کجای دنیا سکونت دارد و غیره. او تنها به دنبال نشر هرچه گسترده‌تر برنامه آلوده خود است.

مثلا فردی یک «کرم» کامپیوتری را تولید و در شبکه رها می‌کند. یک برنامه آلوده به یک بازی رایگان کامپیوتری الصاق می‌شود. یک ویروس برای تلفن‌های هوشمند آندروید ارسال می‌شود. قربانیان از پیش انتخاب نشده‌اند. حتی در موارد بسیاری، هکرها ممکن است تولیدکننده کد مخرب نباشند و فقط از طریق اسکنرهای قدرتمند آسیب‌پذیری‌های امنیتی، محدوده گسترده‌ای از IPها را بررسی و سیستم‌های آلوده و آسیب‌پذیر را شناسایی کنند و هدف حملات سایبری قرار دهند.

• کامیار یک بازی کامپیوتری رایگان را دانلود می‌کند.

کامپیوتر امیر به ویروس Kenzero که در بازی جاسازی شده بود، آلوده شده است. ویروس تمام تاریخچه وب شما و همه سایت‌هایی را که به آن سر زده‌اید با اسم و مشخصات شما در یک سایت آنلاین برای مشاهده همگان منتشر می‌کند. اگر خواستار پاک شدن آن اطلاعات شوید باید ۱۵۰۰ پِن بپردازید!

• امیر از یک فایل کرک برای شکستن قفل نرم‌افزار فتوشاپ برای مکینتاش استفاده می‌کند.

کامپیوتر کامیار به تروجان یا اسب تروایی موسوم به OSX.Trojan.iServices.B که در برنامه کرک جاسازی شده، آلوده شده است. این تروجان بلافاصله از طریق دو گذرگاه (Port) کامپیوتر کامیار را در اختیار حمله‌کنندگان قرار می‌دهد، آنها به راحتی وارد کامپیوتر او می‌شوند و هر مدرک و سندی را که بخواهند دانلود می‌کنند. آنها حتی می‌توانند برنامه‌ای نصب کنند که در هنگام خرید اینترنتی مشخصات کارت اعتباری کامیار را ضبط و برای حمله‌کنندگان ارسال کند. وقتی سیستم به تروجانی آلوده می‌شود، بخش عمده‌ای از کنترل آن به طور بالقوه می‌تواند در اختیار نفوذگران قرار گیرد.

• نگین سایتی را که در آن وعده فروش آی‌پد به قیمت ۹۹ دلار داده شده است، باز می‌کند.

بلافاصله پس از ورود نگین به سایت، پیامی ظاهر می‌شود با این مضمون که کامپیوتر شما به شدت آلوده است و باید از چند ویروس و برنامه آلوده پاک شود، نگین به پیام اعتماد می کند و آنتی ویروس Win 7 Anti-Spyware 2011 را نصب می‌کند. این آنتی ویروس در حقیقت خود یک «ویروس در لباس ضدویروس» است و کنترل کامپیوتر نگین را در دست می‌گیرد.

قربانی انتخاب‌شده و هدفمند

در این نوع حملات، قربانی کاملا انتخاب شده است، حمله به صورت هدفمند صورت می‌پذیرد، حمله‌کنندگان می‌توانند با هدف تخریب روحیه و یا تخریب سیستم‌های سخت‌افزاری و نرم‌افزاری قربانی، سرقت اطلاعات او و یا کنترل و مشاهده فعالیت‌های قربانی، دست به این‌گونه حملات بزنند.

• شما یک ایمیل حاوی یک فایل ورد با فرمت doc. یا docx. دریافت کرده‌اید.

در پاییز سال ۱۳۹۰، ایمیلی که آدرس فرستندهٔ آن، نام دو تن از فعالان سیاسی تحول‌خواه ایران، آقایان امیرارجمند و افشاری را نشان می‌داد، برای جمع محدودی از فعالان سیاسی دیگر ارسال شد. موضوع این ایمیل انتخابات مجلس شورای اسلامی بود. فایل ورد همراه این ایمیل با فرمت doc. حاوی برنامه بسیار پیچیده و خطرناکی بود که توسط ویروس‌یاب‌های معمولی تشخیص داده نمی‌شد. هر کس این فایل را در کامپیوتر شخصی خود باز می‌کرد، امکان ورود و کنترل کامپیوتر خود را برای حمله‌کنندگان فراهم می‌کرد.

• فردی با ایمیلی که حاوی نام شماست، خود را کارمند بانک یا PayPal معرفی کرده و از شما می‌خواهد تا سریعا به آدرس اینترنتی بانک مراجعه کرده و پسورد خود را عوض کنید.

از آنجا که ایمیل حاوی مشخصات شما و نام بانک شماست، مشخصا شما برای این حمله انتخاب شده‌اید و پیش‌تر بررسی‌های دقیقی راجع به هویت شما انجام شده است. در پس آدرسی که ظاهرا مانند بانک شما به نظر می‌رسد، سایت دیگری قرار دارد که فقط ظاهر آن به بانک شما شبیه‌سازی شده است. اگر شما پسورد خود را آنجا وارد کنید، حمله‌کنندگان بلافاصله به حساب بانکی شما مراجعه و آن را خالی می‌کنند. این نوع حملات به Phishing (فیشینگ) معروف‌اند؛ به دام انداختن کاربران با طعمه‌های جعلی و سرویس‌های تقلبی که فقط ظاهر سرویس‌های رایج مورد استفاده کاربر را دارند، اما پشت پرده فقط نیات خراب‌کارانه نهفته است.

• دو راهب بودایی برای دریافت ویزا به سفارت هند در کابل می‌روند.

کامپیوترهای سفارت هند به همراه سفارت‌های مالتا، رومانی، اندونزی، پاکستان، آلمان، پرتغال، تایوان، تایلند، کره جنوبی، دفتر نخست وزیر لائوس، وزارت خارجه ایران، بنگلادش، لاتویا، اندونزی، فیلیپین، برونئی، باربادوس، بوتان و... همه و همه قربانی و عضو شبکه بزرگی از کامپیوترهایی بودند که توسط نوعی تروجان از داخل چین کنترل می‌شدند. شبکه عظیمی که بعدا شبکه ارواح یا «گوست نت» لقب گرفت. نحوه عمل این شبکه این‌گونه بود: یک ایمیل ظاهرا سالم و دارای اطلاعات مرتبط به سفارتخانه مورد هدف ارسال می‌شد. وقتی ایمیل باز می‌شد، اسب تروا یا تروجان اولیه روی کامپیوتر قربانی نصب می‌شد. این تروجان با دو سرور در چین تماس برقرار می‌کرد و در ورودی به کامپیوتر قربانی را می‌گشود. سرور مستقر در چین تروجان دیگری به نام Gh0st Rat را روی کامپیوتر قربانی نصب می‌کرد. این تروجان کنترل کامل کامپیوتر را در دست می‌گرفت، به طوری که اپراتورهای شبکه ارواح از چین می‌توانستند حتی دوربین یا میکروفن کامپیوتر قربانی را روشن کرده و تمام تحرکات اطراف را ضبط کنند.

تقسیم‌بندی تهدیدهای دیجیتال بر اساس مقصد حمله

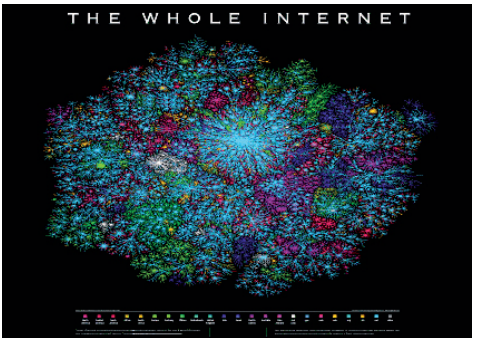
دنیای دیجیتال می‌تواند در سه سطح مورد حمله قرار گیرد:

۱. زیرساخت‌ها و خطوط ارتباطی و ماهواره‌هایی که شهرها، کشورها و قاره‌ها را به یکدیگر متصل می‌کنند.

ساعت دو بامداد روز هشتم آوریل ۲۰۰۹، فردی کابل فیبرنوری شرکت AT&T را در نزدیکی سن‌خوزه و منطقه تکنولوژیک «سیلیکون‌ولی» که در عمق زمین قرار داشت قطع کرد. این عمل منجر به از کار افتادن تلفن، تلفن‌های همراه و اینترنت بسیاری شرکت‌های فعال در منطقه شد. شرکت AT&T برای معرفی مسبب این تخریب ۲۵۰ هزار دلار جایزه تعیین کرد.

در آوریل ۲۰۱۱، یک مادر بزرگ ۷۵ ساله اهل گرجستان، یک کابل ناشناس را در نزدیکی باغ شخصی خود با اره قطع کرد. این عمل موجب قطع کل اینترنت ارمنستان شد.

در ۲۵ دسامبر ۲۰۱۱، کابل فیبر نوری زیردریایی زیر کانال سوئز در مصر، دچار حادثه و آسیب‌دیدگی شد. همین اتفاق برای کابل زیردریایی مشابهی در ایالت تامیل‌نادو هند که هند را به سنگاپور وصل می‌کرد، تکرار شد. این حوادث منجر به ایجاد اختلال جدی در جریان انتقال داده‌ها و پائین آمدن سرعت برای کاربران در جنوب شرقی آسیا و خاورمیانه، خصوصا امارات متحده عربی شدند.



۲. حملات علیه پدیده‌ای است که ما آن را با نام «شبکه جهانی اینترنت» می‌شناسیم.

در این حملات اینترنت مورد حمله قرار می‌گیرد. این حملات می‌تواند در شکل A large scale denial of service attack یا موارد مشابهی باشد که به آن «حملات گسترده تکذیب سرویس» می‌گوئیم. حملات دولت ایران و تلاش برای جعل گواهینامه‌های شرکت Comodo و یا Diginotar، هر دو می‌تواند حمله علیه اساس اینترنت تلقی شود، چرا که به خطر افتادن امنیت گواهینامه‌های اس‌اس‌ال پیامدهای منفی سراسری دارد. این گواهینامه‌ها پایه سیستم احراز هویت و تضمین امنیت در معماری کنونی وب هستند و هر اقدامی بر ضد آن، به طور بالقوه می‌تواند نتایج ویرانگری برای آینده اینترنت به عنوان «شبکهٔ شبکه‌ها» داشته باشد.

۳. حملات علیه برنامه‌های کاربردی (اپلیکیشن‌ها) روی کامپیوترها و تلفن‌های هوشمند متصل به اینترنت.

در این حملات کاربران معمولی اینترنت هدف قرار می‌گیرند. مرورگر شما کار نمی‌کند. برنامه اسکایپ شما از کار می‌افتد و یا گوگل‌تاک مورد حمله قرار می‌گیرد.

پیشنهاد برای طرح سوال در کلاس درس

اغلب کاربران معمولی و دانشجویان تفاوت عمده‌ای میان حملات سطح دوم و سوم حس نمی‌کنند. کاربران اینترنت مجموعه اسکایپ، یاهو مسنجر، مرورگر گوگل کروم. آی‌تونز و دیگر برنامه‌های کاربردی و اپلیکیشن‌ها را جزئی از اینترنت می‌دانند.

مدرس بایستی به روشنی تفاوت یک برنامه کاربردی با شبکه اینترنت را توضیح دهد. فرض کنید در حال بازی ویدئویی در برابر کامپیوتر هستیم، این بازی یک برنامه کاربردی است. حال به شبکه اینترنت متصل می‌شویم. نرم‌افزار بازی ما، یا برنامه کاربردی (Application) قادر است با جست‌وجو در اینترنت فرد دیگری را که در حال بازی در قاره دیگری است بیابد. این دو برنامه از طریق اینترنت با هم تبادل داده می‌کنند و ما می‌توانیم این بار در مقابل یک فرد حقیقی بازی کنیم. اینترنت مجموعه پیچیده شبکه‌ای است که ارتباط آن دو برنامه کاربردی را با هم فراهم می‌آورد. همین مثال در خصوص اسکایپ و یاهو مسنجر هم صادق است.

مطالعه بیشتر

۱. مطالعه بیشتر درباره مبادله پاکت‌های داده که از اساسی‌ترین مفاهیم اینترنت است و در فصل‌های آینده به درک بهتر نحوه کنترل و سانسور پاکت‌ها کمک شایانی خواهد کرد:

http://www.livinginternet.com/i/ii_rand.htm

۲. مطالعه بیشتر در خصوص پروتکل ۱۸۲۲:

http://www.bitsavers.org/pdf/bbn/imp/BBN1822_Jan1976.pdf

۳. مطالعه بیشتر در مورد داستان سوت Cap'n Crunch:

http://www.webcrunchers.com/

۴. ماجرای Kevin Mitnick:

http://news.cnet.com/8301-1009_3-9995253-83.html

۵. منابع مربوط به طبقه‌بندی تهدیدها:

الف. جنگهای سایبری:

http://foreignaffairs.house.gov/112/Fis041511.pdf

ب. جاسوسی سایبری:

http://graphics.thomsonreuters.com/11/04/CyberEspionage.pdf

ج. تروریسم سایبری:

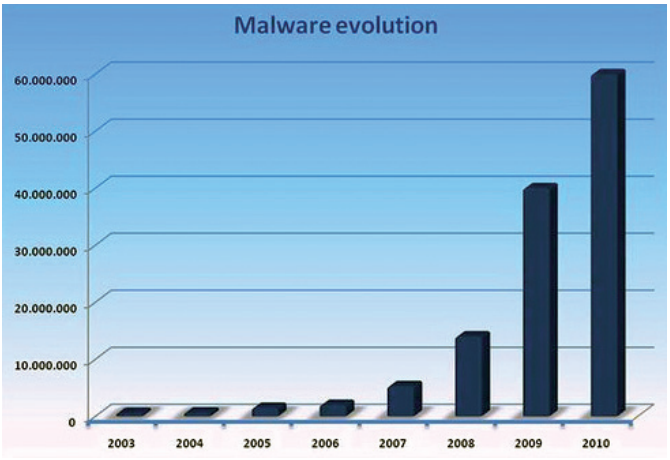
http://www.symantec.com/avcenter/reference/cyberterrorism.pdf

د. جنایات سایبری:
http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf
ه. تخریب:
http://www.cbsnews.com/htdocs/pdf/Cyberbullying_Pages_128_132.pdf
و. هکتیویسم:
http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf

۲
افق تهدیدها

تهدیدها همواره ارتباط مستقیمی با سیر و جهت‌گیری دنیای سایبر دارند. مثلا اگر سال آینده، شاهد ادامه رشد انفجارگونه شبکه‌های اجتماعی باشیم طبعا شاهد حملات و ترفندهای بسیاری برای سرقت اطلاعات کاربران در شبکه‌های اجتماعی نظیر فیس‌بوک خواهیم بود.

علی‌رغم تلاش گسترده شرکت‌های خدمات امنیت کامپیوتری و همچنین امکانات نوظهور امنیتی، بدافزارها به رشد انفجارگونه خود ادامه خواهند داد. نمودار زیر از شرکت امنیتی پاندا، شمار بدافزارهای نوظهور در هر سال را نشان می‌دهد و به‌روشنی گویای وضعیت تهدیدکننده ارائه بدافزارها در سال‌های پیش روست.



آنچه در پیش‌بینی بسیاری از صاحب‌نظران از تهدیدها در سال آینده تکرار می‌شود، این موارد است:

- ادامه تهدید مهندسی اجتماعی (Social Engineering) روی شبکه‌های اجتماعی
- شیوع و رواج ویروس‌های موبایل خصوصا با رواج سیستم‌های پرداخت توسط موبایل
- ادامه افزایش شمار بدافزارها و خصوصا تروجان‌ها
- ظهور ویرس‌های جدید برای دستگاه‌های سیستم عامل مکینتاش (کامپیوترهای شخصی و لپ‌تاپ‌های اپل) و iOS: آی‌فون، آی‌پد و آی‌پاد
- جنگ سایبری و سرکوب دیجیتال، توسط دولت‌های سرکوبگر

حملات عمده اینترنتی

این بخش به ارائه حملات و تهدیدها علیه کاربران اینترنت از آغاز همه‌گیر شدن کاربرد شبکه از دهه ۱۹۹۰ می‌پردازد. ساختار این بخش به این صورت است که حملات مختلف را بر اساس سیر تاریخی آنها ارائه می‌کند. به طور مثال در سال‌های آغازین دهه ۱۹۹۰ حملات مهندسی اجتماعی یا حملات دیگر موسوم به packet spoofing در میان جامعه هکرها بسیار پرطرفدار بوده‌اند و در سال‌های پایانی دهه ۲۰۰۰ حملات موسوم به DDoS (حملات گسترده تکذیب سرویس یا Distributed Denial of Service) اهمیت بیشتری دارند. در این بخش می‌کوشیم با توضیح تعدادی از حملاتی که عمدتا علیه کاربران ایرانی انجام می‌پذیرند، آموزگاران را به مطالعه طیف بسیار گسترده حملات تشویق کنیم.

1990	Packet spoofing
	Hijacking sessions
	Automated probes/scans
	GUI intruder tools
	Automated widespread attacks
	Widespread denial of service attacks
	executable code attacks - browsers
	Techniques to analyze code for vulnerabilities without source code
	Widespread attack on DNS infrastructure
	Widespread attacks using NNTP to distribute attack
	Stealth/advanced scanning techniques
	E-mail propagation of malicious code
	Increase wide-scale Trojan horse distribution
	Distributed attack tools
	DDoS attacks
	Home users targeted
	Anti forensic techniques
	Increase in worms
2012	Sophisticated command and control

Source: SE/CERT CC

برای مطالعه بیشتر درباره حملات بالا، کتاب هک برای Dummies پیشنهاد می‌شود.

نکته مهم: در حال حاضر همه این حملات در سراسر جهان رخ می‌دهند، طبقه‌بندی زمانی ما فقط به این معناست که کدام نوع از حمله، خسارات بیشتری را به بار آورده است.

مهندسی اجتماعی[1] و فریب

مهندسی اجتماعی یا فریب از نخستین تهدیدهای دنیای مجازی به شمار می‌آید و حتی تا امروز در زمره اساسی‌ترین تهدیدها باقی مانده است. مهندسی اجتماعی مبتنی بر دروغ و تقلب است. مهندسی اجتماعی طراحی و اجرای روش‌هایی است که شما و یا فعالان همکار شما را وا دارد تا داوطلبانه تمام و یا بخشی از اطلاعات مورد نیاز نفوذگران را در اختیار ایشان قرار دهند.

مهندسی اجتماعی در واقع زیرساختی برای انواع گوناگون حملات سایبری است که با بررسی نیازهای روز کاربران در شرایط مختلف انجام می‌شود. هکرها تلاش می‌کنند تا با طراحی دام‌های گوناگونی که بیشترین احتمال را برای برانگیختن حس کنجکاوی و عطش اطلاعاتی در کاربران دارند، زمینه سرقت اطلاعات را فراهم کنند. در ادامه با ارائه مثال‌هایی روشن ماهیت این شیوه را تشریح خواهیم کرد.

کاربرد مهندسی اجتماعی برای اخذ اطلاعات و نفوذ داخل سیستم، توسط شیوه‌هایی به شرح ذیل اعمال می‌گردد:

دروغ‌گویی

در بسیاری از موارد با می‌توان افراد را با چند دروغ ساده فریفت و زمینه دسترسی به اطلاعات ایشان را فراهم آورد. یک مثال بسیار ساده به دست آوردن رمز عبور ایمیل شماست. بسیاری از افراد به سادگی، تاریخ تولد، شهر محل تولد و دیگر اطلاعات به ظاهر غیرحساس را در صفحات فیس‌بوک خود منتشر کرده یا در هنگام چت در اختیار افراد ناشناس قرار می‌دهند. بدون آنکه تصور کنند با در دست داشتن این اطلاعات، خرابکار سایبری می‌تواند به سرویس ایمیل شما مراجعه کرده و با ادعای گم کردن رمز عبور، رمز عبور جدیدی دریافت کند.

الف. دروغ‌گویی به شیوه مقام مسئول

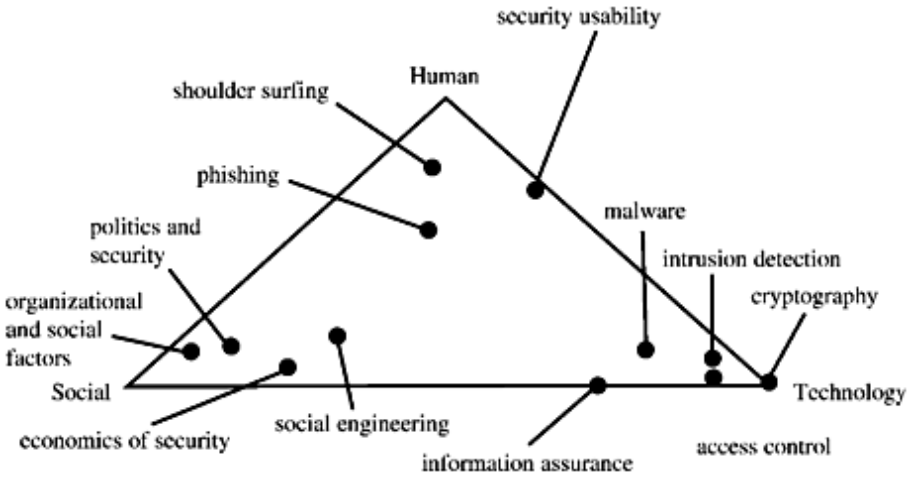
در این روش هکر خود را به جای یکی از مسئولان موسسه یا گروه شما جا می‌زند و خواستار دسترسی به اطلاعات موسسه می‌شود. به طور مثال در چت با شناسه رئیس یک روزنامه اینترنتی وارد شده و از مسئول فنی می‌خواهد، رمز عبور Password روزنامه را تغییر دهد و رمز جدید را جهت اطمینان و حفظ امنیت برای او ایمیل نمایند.

ب. دروغ‌گویی به شیوه شخص ثالث

در این روش جنایتکاران سایبری، خود را به عنوان کارمندان یک موسسه ثالث جا می‌زنند، مثلا اگر

1. Social Engineering

هاست و دومین شما را دو شرکت مختلف سرویس‌دهی می‌کنند، به عنوان کارمندان شرکت دومین از شما خواستار ارائه اطلاعات مربوط به هاست می‌شوند و یا بالعکس. نمونه ساده آن، روش‌هایی است که سارقان برای ورود به ساختمان شرکت‌ها استفاده می‌کنند؛ پوشیدن لباس شبیه ماموران، برق، تلفن و یا نظافتچی‌ها.



خرابکاری درونی

جنایتکاران برای دستیابی به اطلاعات مورد نیاز خود، قربانی و یا نزدیکان وی را به شیوه‌هایی این‌چنینی تحت فشار قرار می‌دهند تا زمینه همکاری و نفوذ فراهم گردد:

الف. رشوه

به سادگی فرد مورد نظر یا یکی از همکاران او با پرداخت رشوه تطمیع می‌شود تا اطلاعات مورد نیاز را در اختیار آنان قرار دهد، شایان توجه است که پرداخت رشوه غالبا به صورت مستقیم برای دریافت اطلاعات صورت نمی‌گیرد. رشوه به صورت هدیه‌ای غیرمعمول در ازای دریافت کمکی بسیار جزئی و بی‌خطر پیشنهاد می‌شود. آن کمک کوچک زمینه دسترسی جنایتکاران به اطلاعات بعدی را فراهم خواهد کرد. این اطلاعات در فرآیند «مهندسی گام‌به‌گام» تا جایی پیش می‌روند که حدس یا کشف پسوردهای مرتبط برای ورود به محیط‌های مجازی مورد نظر هکر را تسهیل کنند. قربانی ممکن است در این میان نقش چندانی نداشته باشد، اگر چه اشتباهات فاحش کاربران می‌تواند در بسیاری از موارد یاری‌رسان هکرها باشد؛ مثلا اگر پسورد شما شماره گواهی‌نامه یا کارت ملی شما باشد، یا حتی اعداد مرتبط با این شناسه‌های هویتی در پسورد شما گنجانده شود، حدس زدن پسوردها را در فرآیند Crack کردن برای نفوذگران بسیار ساده‌تر خواهد کرد. به همین‌خاطر کاربر باید پسوردها را از میان کلمات و عباراتی کاملا نامربوط و نامرتبط با هویت اجتماعی و حرفه‌ای خود انتخاب کند.

ب. فریب و اغواء

از روش‌های بسیار معمول جنایتکاران، ظاهر شدن در قالبی دروغین، مثلا دختران و زنان جذاب، استفاده از پروفایل جذاب در شبکه‌های اجتماعی و ریختن طرح دوستی و سوء استفاده از احساسات انسانی قربانیان است.

ج. تهدید

تهدید خانواده یا شخص قربانی به خشونت فیزیکی یا از بین بردن اموال ایشان از روش‌های معمول تبهکاران است. این روش در حکومت‌های سرکوبگر به صورت گسترده به کار گرفته می‌شود. در سال ۲۰۰۴ گروهی از وبلاگ‌نویسان ایرانی بازداشت شدند. بازجویان با حبس آنان در سلول‌های انفرادی، شکنجه و ضرب و شتم ایشان، تهدید به تجاوز و شکنجه خانواده، ازآنان خواستار اطلاعات فنی، رمزهای عبور و دیگر مشخصات سایت‌های اینترنتی منتقد شدند. اطلاعاتی که به طور بالقوه غیر از خود زندانیان، بسیاری از دوستان و همکاران آنها را هم در معرض خطرات جدی قرار داد و همچنان می‌دهد. کسب این اطلاعات، به تکمیل پازل‌های اطلاعاتی درباره افراد دیگر نیز کمک شایانی می‌کند و زمینه را برای سرکوب افراد، نهادها و شبکه‌های حرفه‌ای و اجتماعی دیگر نیز فراهم می‌سازد.

د. باج‌گیری

باجگیری با تهدید قربانیان به افشای عمومی اطلاعات خصوصی و اسرار آنان صورت می‌پذیرد؛ به طور مثال تبهکاران با دست‌یابی به فیلم یا تصاویر بسیار خصوصی افراد، آنان را تهدید می‌کنند که در صورت عدم همکاری، این تصاویر در اختیار نزدیکان، اعضای خانواده و یا افکار عمومی قرار خواهد گرفت.

علاوه بر تهدیدهای ذکر شده در بالا، نفوذ به سازمان و یا نهاد شما می‌تواند به سادگی با نفوذ شخصی تبهکاران به عنوان عضو، هوادار، داوطلب و غیره صورت پذیرد. خصوصا در مواردی که افراد ناشناس بدون استفاده از نام حقیقی و با شناسه مجازی فعالیت می‌کنند. در سال ۲۰۱۰ جمعی از فعالان اینترنتی ایران در جلسه‌ای خصوصی تصمیم گرفتند سایتی اینترنتی با نام «ایران رسا» تاسیس کنند. ساعتی پس از پایان این جلسه، تمام دامنه‌های ایران رسا توسط سازمان‌های اطلاعاتی ایران رجیستر شده بود. این نمونه، نفوذ بسیار ساده تبهکاران به گروه‌های فعال را در قالب داوطلب و هوادار به نمایش می‌گذارد.

مثال‌هایی متداول از روش‌های مهندسی اجتماعی

• ایمیل‌های معروف به ۴۱۹ یا نیجریه: فردی برای شما یک ایمیل می‌فرستد و ادعا می‌کند میلیون‌ها دلار سرمایه یکی از افراد معروف در گذشته – مثلا موبوتو – در بانک‌های سوئیس است و او به کمک شما می‌تواند این سرمایه عظیم را به آفریقا منتقل کند. او در برابر، نصف این پول را به شما خواهد داد؛ اگر مایلید مدارک حساب را برای شما ارسال کنند، مثلا ۵۰ دلار برای او بفرستید.

• ایمیل‌های مشهور به پیش‌پرداخت: در این مورد، برای یکی از شرکت‌کنندگان دوره دوم امنیت سایبری، نامه‌ای ارسال شده بود که متن آن را در کادر زیر می‌بینید:

----- Forwarded Message -----
From: U.S. Department of State <dv@greencard-org.com>
To: XXX
Sent: Tuesday, September 6, 2011 3:04 PM
Subject: U.S. Department of State - United States Permanent Resident Card for XXX

Your registered name XXX is included to show this message originated from U.S. Department of State. U.S. Department of State notifies XXX of being selected as a winner of the Diversity Visa program.

Dear XXX, You are one of the 50,000 winners selected by the computer random draw from the 12.1 million entries registered in the Diversity Immigrant Visa Program . The Diversity Immigrant Visa program is a United States congressionally-mandated lottery program for receiving a United States Permanent Resident Card. It is also known as the Green Card Lottery.

Processing fees

Type of Residence Card Status Amount (per person) United States Permanent Resident Card Granted! - Waiting for payment of processing fee $879 Processing fees Included Total $879 Although the Diversity Visa participation was free, the law and regulations require to every diversity visa winner to pay a visa processing fee of $879. The Diversity Visa(Green Card) is guaranteed upon receiving the payment.

The per person fee for each Diversity Visa is $879, payable in U.S. dollars or equivalent of your local currency. This $879 fee is the only fee a winner needs to pay throughout the entire relocation process.

Accompanying family members(wife/husband, fiancee, brothers, sisters, childrens, cousins) may be included in the program and their visas will be provided at the same time with yours so you can travel/move together in the same time. However the fees must be paid per person and each member(e.g wife, brother, parents, childrens, cousin) must pay $879. There is no discount for childrens.

Please note that you are allowed to take with you as many family members you want. However for each person you must pay an additional amount of U.S $879

For example if you decide to move in the United States with your wife and a kid the total fee is US$879(your fee) + US$879(your wife) + US$879(your kid) = US$2637.

همان طور که در ایمیل به روشنی مشاهده می‌کنید، تبهکار اینترنتی خواستار ارسال ۸۷۹ دلار پیش‌پرداخت برای ارسال گرین‌کارد شما شده است. چنین ترفندی در اشکال مختلف – مثلا شما یک آی‌فون و یا آی‌پد برنده شده‌اید و... – ارسال می‌شود. تبهکاران عمدتا ایمیل قربانیان را از سایت‌های بخت‌آزمایی مثلا «برای برنده شدن در گرین کارد اینجا را کلیک کنید» و «اگر یک آی‌فون می‌خواهید اینجا را کلیک کنید» به دست می‌آورند.

ترفند دیگر، فیشینگ است که بعدا به تفصیل توضیح داده خواهد شد. در فیشینگ تبهکاران خود را به جای بانک شما، یا سرویس دهنده ایمیل شما جا زده و از شما می‌خواهند به سایتی بروید که ظاهر آن شباهت زیادی به سایت اصلی بانک یا ایمیل شما دارد. اما این شباهت‌ها فقط ظاهری است. در آن سایت

ناشناس، تبهکار از شما می‌خواهد ایمیل و پسورد خود را وارد کنید. هدف او دستیابی به این اطلاعات است. البته اگر دقت کافی داشته باشید، از روی آدرسی که در آدرس‌بار مرورگر شما ظاهر می‌شود و با مقایسه آن با آدرس‌های واقعی مثلا سرویس ایمیل خود که همیشه می‌بینید، می‌توانید به سادگی جعلی بودن محیط شبیه‌سازی‌شده را تشخیص دهید، گرچه نفوذگران همه تلاش خود را می‌کنند که از این نظر هم بیشترین شباهت ممکن را در برابر چشمان شما بگذارند.

مقابله با روش‌های مبتنی بر مهندسی اجتماعی

مقابله با روش‌های مبتنی بر مهندسی اجتماعی، نیازمند پیش‌بینی، دقت، مصون‌سازی و آموزش است. در این بخش می‌کوشم تا با ذکر مثال‌هایی واقعی به ایجاد نوعی «درک مقابله با تهدیدهای مبتنی بر مهندسی اجتماعی» کمک کنم.

توصیه اول: این سوال را چند بار از خود بپرسید: او واقعا همان کسی است که ادعا می‌کند؟

در هنگام مواجهه با یک دوست جدید اینترنتی، یک پیام، یک ایمیل حاوی درخواست دوستی، یک تصویر و یا ارتباط اتفاقی اسکایپ، بدون هیچ رودربایستی سوالات زیر باید پرسیده شود؟ آیا شما را می‌شناسم؟ قبلا شما را دیده‌ام؟ از کجا شناسه و اطلاعات تماس مرا یافتید؟ این سوالات نیازمند جواب روشن و بدون ابهام هستند.

پاسخ اول: «بله؛ من محمد امیری، هم‌کلاسی شما در دانشکده کامپیوتر دانشگاه علم و صنعت ایران، ورودی ۱۳۸۰ هستم!» این پاسخ نوعی پاسخ قابل قبول تلقی شده و وظیفه بعدی تحقیق درباره صحت این ادعا خواهد بود.

پاسخ دوم: «چطور منو نمی‌شناسی؟ چه اهمیتی داره کی هستم؟ حالا یک کم گپ بزنیم خودت می‌فهمی من کی هستم!» این نوع پاسخ‌ها، پاسخ غیرقابل قبول هستند. تنها واکنش به این نوع درخواست، قطع ارتباط بدون هیچ توضیح اضافی است.

موضوع بسیار حائز اهمیت در مقابله با این روش‌ها توجه به دو نکته در شیوه‌های حرفه‌ای کسب اطلاعات توسط تبهکاران و یا عوامل دولت‌های سرکوبگر است:

نکته اول: آنان همه اطلاعات را به یک‌باره نمی‌گیرند؛ با شما طرح دوستی می‌ریزند و در طی زمان، گام به گام پازل اطلاعاتی خود را کامل می‌کنند. اگر برای دسترسی به سیستم شما نیازمند ۸ قلم داده، از قبیل تاریخ تولد، محل تولد و... باشند، به صورت زمان‌بندی‌شده و مثلا با ارتباط چت در طول زمانی طولانی این داده‌ها را یک به یک از شما اخذ می‌کنند. حتی ممکن است افراد مختلفی مامور ارتباط با شما شده و هر یک به دنبال قطعه‌ای از این پازل باشند.

نکته دوم: تخلیه اطلاعاتی با سوء استفاده از سهل‌انگاری شما، هدف تبهکاران است. فرض کنید تبهکار شماره موبایل شما را در اختیار داشته، قصد دسترسی به اطلاعات پرسنلی شما نظیر آدرس، محل تولد، تاریخ تولد، شماره شناسنامه و... را دارد. مکالمه احتمالی به این شکل خواهد بود: «الو سلام؛ از دانشگاه آزاد واحد تهران مرکزی تماس می‌گیرم، من نجفی هستم،

همکار آقای سعیدلو، مسئول بایگانی اداره آموزش (سعیدلو فردی است که واقعا وجود دارد و برای بالابردن اعتبار مکالمه از او یاد می‌شود)، پرونده شما مقداری اطلاعات کسر دارد، محبت می‌کنید سوال‌های من را جواب بدهید؟» مقابله با تهدید مکالمه بالا نیازمند قدری آموزش است. کافی‌ست شما سوال فوق را اینچنین جواب دهید: «بله؛ خواهش می‌کنم، لطف کنید شماره تلفن و داخلی‌تان را بدهید. من با شما تماس می‌گیرم.»

مقابله با اخذ اطلاعات به شیوه‌هایی نظیر تهدید، ارعاب و شکنجه

در مناطقی از جهان که پلیس و نیروهای امنیتی، ضابطین قانونی و مدافع حقوق شهروندان آزادند، بهترین راه حل، مراجعه به پلیس و استفاده از ظرفیت‌های حرفه‌ای سازمان‌های امنیتی در مقابله با جنایت سازمان‌یافته سایبری است. اما متاسفانه در برخی مناطق جهان نیروی پلیس، خصوصا پلیس سیاسی و امنیت، خود بخشی از جنایت سازمان‌یافته سایبری است.

رعایت مواردی از این دست می‌تواند، بسیاری از تهدیدهای جدی از ناحیه نیروهای سیاسی سرکوبگر را خنثی نماید:

هنگامی‌که چت می‌کنید، لحظاتی را در نظر آورید که یک بازجو، متن کامل لغاتی را که در حال تایپ کردنش هستید، به صورت پرینت جلوی شما می‌گذارد. این بازجو می‌تواند فردی باشد که همین حالا مشغول چت کردن با او هستید. این بازجو می‌تواند بالای سر دوستی که در حال حاضر با او چت می‌کنید ایستاده باشد و این بازجو می‌تواند به راحتی شیشه اتومبیل دوست شما را شکسته، کامپیوتر نوت‌بوک او را دزیده و از قسمت آرشیو چت ایمیل دوست شما، تمام متن چت شما را پرینت کند. چت متنی از ناامن‌ترین شیوه‌های ارتباط آنلاین است. اگر از سرویس چت شبیه Gmail استفاده می‌کنید، حتما آرشیو چت را غیرفعال کنید و با افرادی که احتمال می‌دهید، متن چت را جایی ذخیره می‌کنند و یا امکان آرشیو را غیرفعال نکرده‌اند، چت نکنید. در صورت غیرفعال نبودن آرشیو چت جی‌میل، حتی اگر از میانه مکالمه روی گزینه Off the Record کلیک کنید، متن چت در اکانت هیچ‌یک از دو سوی ارتباط ذخیره نخواهد شد.

اگر در ایران زندگی می‌کنید باید بدانید و کاملا درک کنید که در یکی از خطرناک‌ترین مناطق کره زمین به دنیا آمده‌اید و در حال زندگی هستید. اکثریت ساکنان کره زمین حتی در مناطق کمتر توسعه‌یافته نظیر آفریقا، باور نخواهند کرد که در کشور شما، افراد به دلیل نوشیدن یک قوطی آبجو یا نشستن کنار دوست‌دخترشان در پارک مجازات، حبس و حتی محکوم به تحمل شلاق خواهند شد. همچنین بسیاری از ایرانیان نمی‌دانند که بر اساس قوانین جاری ایران، مجازات سه بار نوشیدن مشروبات الکلی اعدام است. به عنوان یک کاربر اینترنت متاسفانه شما نمی‌توانید در قلمرو جمهوری اسلامی ایران زندگی کنید و تصاویر میهمانی جشن تولد خود را

مانند یک جوان ساکن آنگولا، اردن و یا ترکیه روی فیس‌بوک و یا وبلاگ خود قرار دهید؛ شما را با این تصاویر مورد فشار و شکنجه قرار خواهند داد.
سیستم‌های امنیتی جمهوری اسلامی ایران از نوعی پارادوکس انسانی - غیرعقلانی نهایت استفاده را می‌کنند. آنان می‌دانند بسیاری از فعالان اینترنتی، دانشجویی، روزنامه‌نگاران و منتقدان سیاسی، شیوه زندگی مدرنی دارند. آنان می‌دانند که برخی از این افراد مانند آدمیان دیگر، از مشروبات الکلی استفاده می‌کنند و یا روابط جنسی خارج از ازدواج دارند. در کشور ایران از این اطلاعات برای تحت فشار قرار دادن منتقدان استفاده می‌شود. لذا اکیدا از فیلمبرداری، تصویربرداری، خاطره‌نویسی و شرح این نوع روابط برای دیگران بپرهیزید. در شرایط کنونی اکثر تلفن‌های همراه قابلیت ضبط فیلم را دارند. هنگامی که مشغول ضبط فیلم با تلفن همراه خود و یا از طریق وب‌کم کامپیوتر خود هستید، باید بدانید که دو نفر موتورسوار به راحتی قادرند تلفن همراه شما را در هنگام صحبت در خیابان، قاپ بزنند و از دست شما احتمالا هیچ کاری ساخته نیست.
فیلم، صدا، مکالمات تلفنی آخر شب با شریک عاطفی، شرح پارتی و دخیره و انتشار عکس‌های خصوصی، طلایی‌ترین فرصت‌ها را برای تحت فشار قراردادن شما در اختیار بازجو و پلیس سیاسی قرار می‌دهد.

یک شیوه موثر اگر احتمال بازداشت خود را می‌دهید، ذخیره داده‌های مهم و حساس در یک سرویس اینترنتی آنلاین نظیر گوگل و یا فضاهای ذخیره امن و مطمئن در فضای مجازی است. رمز عبور این داده‌ها را به همراه سوال‌های امنیتی برای تغییر رمز (Security Questions and Password hint) می‌توانید در اختیار فرد مورد اعتماد خود در خارج از ایران قرار دهید تا بلافاصله پس از بازداشت احتمالی شما همه رمزهای عبور را تعویض نماید. سرعت عمل این فرد بسیار مهم و حیاتی است. چرا که شما غالبا می‌توانید در مقابل بازجویان برای یک یا چند روز نخست مقاومت کنید.

بسته‌های داده قلابی[1]

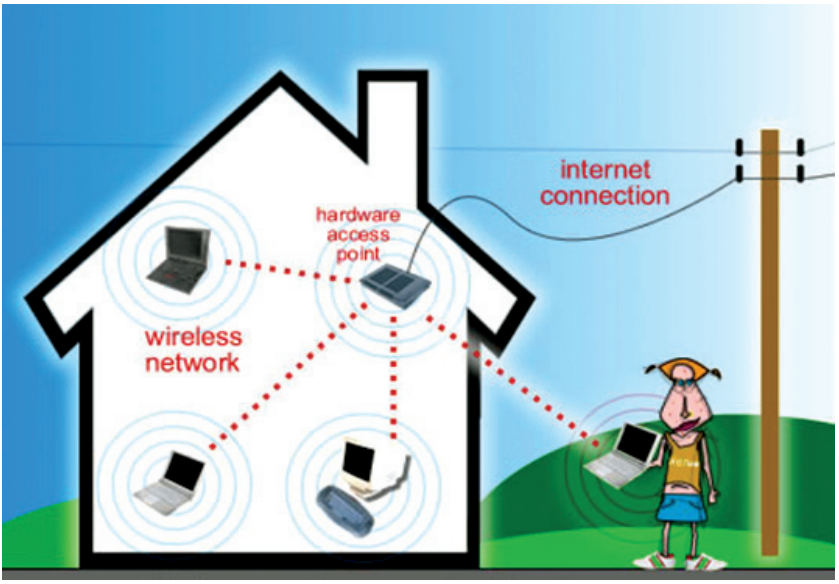
Spoofing و Sniffing دو روش بسیار معمول مورد استفاده هکرها در سال‌های آغازین حملات اینترنتی‌اند که کاربرد آنها تا به امروز ادامه یافته است.

Sniffing یا بوکشیدن به مانند سگ‌های شکاری، تجزیه و تحلیل اطلاعات در جریان میان اجزای مختلف شبکه است. ابزارهای کلاسیک Sniffing که به آن‌ها Sniffer گفته می‌شود سال‌هاست مورد استفاده متخصصان امنیت سایبری برای شناسایی نقاط ضعف شبکه‌ها و همچنین مورد سوءاستفاده هکرهاست. نرم افزار Wireshark یکی از مشهورترین این ابزارهاست.

بسته به بخشی از شبکه که در آن بوکشیدن و تحلیل پاکت‌های داده انجام می‌پذیرد، می‌توانیم

1. Packet spoofing

Ethernet sniffer یا Wireless sniffer داشته باشیم، تصویر زیر فردی را نشان می‌دهد که با یک لپ‌تاپ در کنار منزل مسکونی که در آن یک شبکه وایرلس ناامن وجود دارد در حال نفوذ به شبکه خانگی و دستیابی به اطلاعات کامپیوترهای متصل به شبکه است.



Spoofing: به هنگام تبادل داده‌ها میان اجزاء شبکه، در سربرگ یا header پاکت‌های داده، اطلاعاتی مربوط به فرستنده پاکت داده وجود دارد، Spoofing دست‌کاری این داده‌ها به نحوی است که شما خود را به جای فرستنده پاکت داده جا بزنید و طبعا کامپیوتر دریافت کننده پاکت داده به جای شما، به دستگاهی که خود را به جای او جا زده‌اید پاسخ خواهد داد. نوعی جعل هویت با بهره‌گیری از نرم‌افزارها و با سوء استفاده از آسیب‌پذیری‌های امنیتی موجود در شبکه‌های اطلاعاتی، برای نفوذ به جریان تبادل داده‌ها و مدیریت آن در برهه‌های زمانی مشخص، با هدف کسب اطلاعاتی که ممکن است در آینده علیه یک یا هر دو سوی این ارتباط آنلاین مورد استفاده قرار گیرد.

برای مطالعه بیشتر این لینک پیشنهاد می‌شود:

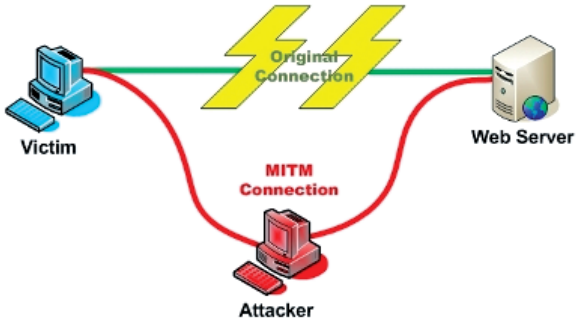
http://www.cis.syr.edu/~wedu/seed/Labs/Sniffing_Spoofing/Sniffing_Spoofing.pdf

دزدیدن ارتباط یا جلسه[1]

آشنایی با ماهیت این دسته از حملات برای کاربر اینترنتی در ایران از اهمیت بسیار بالایی برخوردار است چرا که بسیاری از حملات با پشتیبانی دولت ایران در این طبقه‌بندی قرار می‌گیرند. این حملات

1. Session Hijacking

عبارت‌اند از حاضر بودن یک نفر سوم در میان راه ارتباط «عمدتا امن» کامپیوتر شما و یک کامپیوتر دیگر مثلا سرورهای شرکت گوگل، زمانی که شما جی‌میل خود را چک می‌کنید.



برای توضیح حملات موسوم به «دزدیدن ارتباط یا جلسه» برای دانش‌آموزان از مثال ساده زیر استفاده کنید:

• آرش وارد اکانت خدمات الکترونیکی بانک خود می‌شود. به صورت بسیار ساده ارتباطی میان کامپیوتر بانک و کامپیوتر آرش برقرار می‌شود. کامپیوتر سوم یا همان مهاجم دیگری که قصد دزدیدن اطلاعات بانکی آرش را دارد وارد جلسه میان آرش و بانک می‌شود. خود را به جای آرش جا می‌زند و به اطلاعات بانکی او دست پیدا می‌کند.

• مهتاب اکانت جیمیل خود را چک می‌کند. فردی برای او یک ایمیل فرستاده است. فایل word به این ایمیل attach یا الصاق شده است، این فایل آلوده به نوعی کد مخرب و مهاجم است. این کد در کامپیوتر مهتاب به انتظار می‌نشیند، به محض اینکه مهتاب وارد جی‌میل خود می‌شود، کد به «cookies» جی‌میل دسترسی پیدا می‌کند. در حقیقت مهاجم در اینجا با استفاده از یک کد نه چندان پیچیده و با استفاده از ضعف‌ها و آسیب‌پذیری‌های احتمالی جی‌میل، ارسال و دریافت اطلاعات میان کامپیوتر مهتاب و جی‌میل را کنترل می‌کند. این اطلاعات برای مرکز کنترل فرد یا سازمان مهاجم ارسال می‌شود، فرد مهاجم پسورد جی‌میل مهتاب را به دست می‌آورد. او می‌تواند این پسورد را تغییر دهد و مانع از دسترسی مهتاب به پست الکترونیکی خود شود.

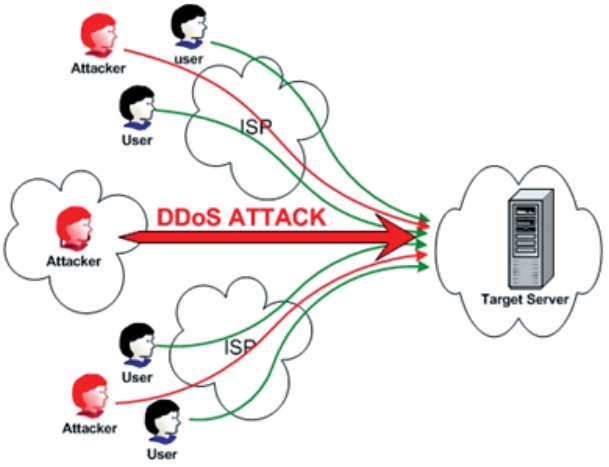
توضیح: جی‌میل ظاهرا این مشکل را حل کرده است.

حملات قطع و توقف سرویس[1]

حملات موسوم به قطع و توقف سرویس در اشکال بسیار متفاوت اما با راهبردی تقریبا یکسان سازماندهی می‌شوند؛ سرازیر کردن تعداد بسیار زیادی درخواست تبادل داده با یک عضو شبکه به حدی

1. Denial of service attacks

که تمام امکانات آن عضو شبکه اشغال شده و از دسترس خارج شود. مثلا اگر سرور یا سایتی امکان پاسخگویی و بازدید همزمان ۵۰۰۰ بازدید کننده را داشته باشد، طبعا اگر ۵۰ هزار بازدید کننده در آن واحد از سرور یا سایت، تقاضای بازدید کنند، سرور که ظرفیت پاسخگویی به همه این درخواست‌ها را ندارد از دسترس خارج خواهد شد. DDoS یا Distributed denial-of-service attacks نوعی از همین خانواده حملات هستند که در آن تعداد بسیار زیادی کامپیوتر مختلف در مکان‌های متفاوت و بعضا از چند قاره، هم‌زمان سرور یا کامپیوتر خاصی را به صورت مدیریت شده هدف قرار می‌دهند.



چند مثال برای کمک به توضیح بیشتر برای دانشجویان:

• در میانه تظاهرات خونین اعتراض به نتایج آراء سال ۱۳۸۸ در ایران، هزاران کاربر ایرانی با استفاده از امکانی به نام http://pagereboot.com/ همزمان مثلا به سایت فارس نیوز رفتند و Pagereboot خود را برای رفرش کردن صفحه هر دو ثانیه یکبار تنظیم کردند. نتیجه این عمل دسته جمعی، سقوط فارس نیوز بود، چرا که فرض کنید فارس نیوز می‌بایستی هر دو ثانیه به ده هزار request یا درخواست جدید ارسال اطلاعات، به صورت هم‌زمان پاسخ می‌داد. فارس نیوز در واکنش به این اقدام کاربران، به این شکل به حملات پاسخ داد: آنها requestهای جدید را به سایت بالاترین هدایت کردند و در نتیجه با هر حمله جدید، حمله به طور هدایت شده به سرورهای بالاترین منتقل می‌شد.

• روز هفت فوریه سال ۲۰۰۰ هکری به نام Mafiaboy سایت چند بیلیون دلاری یاهو را با یک سلسله حملات DDoS برای مدت نزدیک به یک ساعت از کار انداخت. او در خلال هفته بعد از این عملیات سایت‌های Amazon، Ebay، CNN و Dell را توسط حملات DDoS از کار انداخت و میلیون‌ها دلار خسارت را موجب شد. هکرهای ناشناس (Anonymous) هم عموما از همین شیوه برای تحقق اهداف خود در جهان مجازی بهره می‌گیرند.

اگر قصد راه‌اندازی یک وب‌سایت منتقد که احتمال حملات DDoS علیه آن می‌رود را دارید، ناگزیر از رعایت نکات زیر هستید:

• میزبانی وب‌سایت خود را به هاستی که خدمات حفاظت در برابر DDoS را ارائه می‌کند بسپارید.

• با مشورت با متخصصین امنیت وب، یک برنامه کامل و مسنجم برای مواجهه با حملات DDoS تدوین کنید.

• چند متخصص امنیت وب را در دسترس داشته باشید تا در صورت حمله DDoS، به شما کمک کنند؛ از آنان بخواهید تنها از روش‌های قانونی و اخلاقی برای پاسخ به حملات استفاده کنند.

حملات قطع و توقف سرویس با استفاده از بات نت‌ها[1]

بات‌نت‌ها مجموعه گسترده‌ای از کامپیوترهایی هستند که توسط یک کامپیوتر مرکزی کنترل می‌شوند. کامپیوتری که گروه را به راه انداخته و دیگر کامپیوترها را کنترل می‌کند «Bot herder» یا «Bot master» نامیده می‌شود و کامپیوترهای دیگری که از راه دور در اختیار او قرار گرفته‌اند اصطلاحا «زامبی» (Zombie) خوانده می‌شوند.

سوال: بات‌نت‌ها به چه کار می‌آیند؟

• بات‌نت‌ها مثلا برای ارسال اسپم یا هرزنامه به کار می‌روند. سرورهای ایمیل معمولا اگر از یک کامپیوتر چند صد هرزنامه ارسال شود، آن نامه‌ها را اسپم تلقی می‌کنند. برای همین فرستندگان اسپم ده‌ها هزار کامپیوتر زامبی را از راه دور به کار می‌گیرند و اسپم خود را به واسطه آنها ارسال می‌کنند.

• مورد دیگر استفاده از بات‌نت‌ها، نبردهای سایبری است. مثلا در جریان جنگ سایبری هکرهای نزدیک به دولت روسیه علیه استونی (۲۰۰۷) یا گرجستان (۲۰۰۸)، هکرهای روسی برای اجرای حملات DDoS از ده‌ها هزار کامپیوتر زامبی مثلا در آمریکای جنوبی استفاده کردند. بدون آنکه کاربران آن کامپیوترها اساسا اطلاعی داشته باشند که کامپیوترشان در حال بمباران سرورهای استونی یا گرجستان است. اگر تمام حملات فرضا از داخل روسیه صورت می‌پذیرفت آن وقت متخصصان دفاع سایبری ناتو در مورد استونی و گرجستان می‌توانستند تمام درخواست‌های با مبدا داخل روسیه را بلوکه کنند. اما با نامتمرکز بودن و پخش کامپیوترهای بات‌نت در سراسر جهان، منشا واقعی حملات تا حدی پشت کامپیوترهای قربانی و اسیر بات‌نت پنهان می‌ماند.

سوال: بات‌نت‌ها چگونه ساخته می‌شوند؟ ساخت بات‌نت سه مرحله دارد:

• یک برنامه آلوده توسط کامپیوتر قربانی دانلود می‌شود، تجربه نگارنده نشان می‌دهد بازی‌های کامپیوتری مجانی و یا نرم‌افزارهای مجانی که از سایت‌های مشکوک دانلود می‌شوند،

1. Denial of service attacks using Botnets

به طرق مختلفی از جمله نصب تروجان‌ها، درهای امنیتی کامپیوتر قربانی را به روی کامپیوتر مهاجمی که تعمدا بازی یا نرم‌افزار مجانی را در اینترنت پراکنده باز می‌کنند. بنابراین ماجرا ساده است؛ حتی شما هم ممکن است بخشی از سیستمی باشید که برای تحقق اهداف خراب‌کارانه بزرگ طراحی شده، بدون آن‌که بدانید!

• کامپیوتر مهاجم منتظر می‌ماند تا ده‌ها هزار کامپیوتر قربانی در اختیار او قرار گیرند.

• از این کامپیوترها در روز موعود برای ارسال اسپم، دست‌کاری موتورهای جستجو، جنگ سایبری و یا تقلب و کلاه‌برداری اینترنتی استفاده می‌شود. یکی از خطرناک‌ترین استفاده‌های بات‌نت‌ها به این شکل است: شماره کارت اعتباری هزاران قربانی سرقت می‌شود و سپس تبهکاران روی کامپیوترهای زامبی و قربانی اقدام به سوء استفاده از کارت‌ها می‌کنند در این صورت پلیس حتی با تعقیب آی‌پی و دسترسی به کامپیوتر قربانی، در حقیقت قربانی دیگری را یافته و نه تبهکار اصلی را.

بسته‌های اکسپلویت[1] یا بهره‌کشی از سیستم‌های هدف

هکرها و موسسات زیرزمینی بسیاری که عموما در فدراسیون روسیه فعالیت دارند، Exploit packها را در شکل بسته‌های نرم‌افزاری با قیمت و سرویس متفاوت ارائه می‌کنند. این بسته‌ها توسط تبهکاران مورد استفاده قرار می‌گیرد تا به کامپیوترهای قربانیان دسترسی پیدا کنند. قیمت این بسته‌ها از چند دلار تا چند هزار دلار متفاوت است و طبعا برای عملیات پیچیده‌تر، فروشندگان بسته‌ها حاضرند در برابر پرداخت وجه، حتی یک سال به تبهکاران سرویس فنی ارائه نمایند. این بسته‌ها اسامی متفاوتی دارند که به دلایل مختلف از ذکر این اسامی در اینجا خودداری می‌شود. علاقه‌مندان می‌توانند از طریق موتورهای جستجو، لیست Exploit packها را به دست آوردند و با شیوه عملکرد آنها بیشتر آشنا شوند.

شرکت امنیت دیجیتال مشهور trendmicro در تازه‌ترین گزارش تحقیقی خود، بهای خرید و یا اجارهٔ ابزارهای هکری در روسیه را منتشر کرده است، برخی از این خدمات به شرح ذیل هستند:

• خرید یک botnet سفارشی به صورت آماده: ۷۰۰ دلار

• اجاره botnet: ساعتی ۲ دلار

• زئوس (کد بسیار قوی برای ایجاد تروجان برای سرقت اطلاعات مالی و ایجاد botnet سفارشی) با هاست: ۴۰۰ دلار

• اسپم: ۱۰ دلار برای ۱ میلیون ایمیل

• روت‌کیت ویندوز: ۲۹۲ دلار

• هک سفارشی جی‌میل، هر ایمیل: ۱۱۶ دلار

• هک سفارشی فیس‌بوک و توییتر: ۱۳۰ دلار

• هک ایمیل شرکت‌ها: ۵۰۰ دلار

1. Exploit packs

- حمله وسیع DDoS روی هر سایت: ساعتی ۳۰ تا ۷۰ دلار، ماهی ۱۲۰۰ دلار
- صدهزار اس‌ام‌اس اسپم: ۱۵۰ دلار

شیوه‌های مرسوم عمل Exploit packها

علی ایمیلی دریافت کرده است که از او می‌خواهد برای دیدن عکس‌های بسیار جالبی به سایتی ناشناس برود، علی با تایپ آدرس وارد سایت می‌شود. گردانندگان سایت، اسکریپتی از یک Exploit pack را در سایت نصب کرده‌اند. وظیفه این اسکریپت آلوده کردن ماشین علی است. مثلا برنامه Adobe Acrobat او هدف قرار می‌گیرد و تکه‌ای کد آلوده به این برنامه که روی اغلب کامپیوترهای شخصی قرار دارد الصاق می‌شود. بسیاری از وب‌سایت‌های آلوده که توسط Exploit packها تولید شده‌اند برنامه کوچکی مثلا KeyLogger را روی کامپیوتر قربانی نصب می‌کنند. کی‌لاگرها نرم‌افزارهایی هستند که همه کلیدهای فشرده شده روی یک سیستم، از جمله username و password را برای دستگاه تبهکاران ارسال می‌کند.

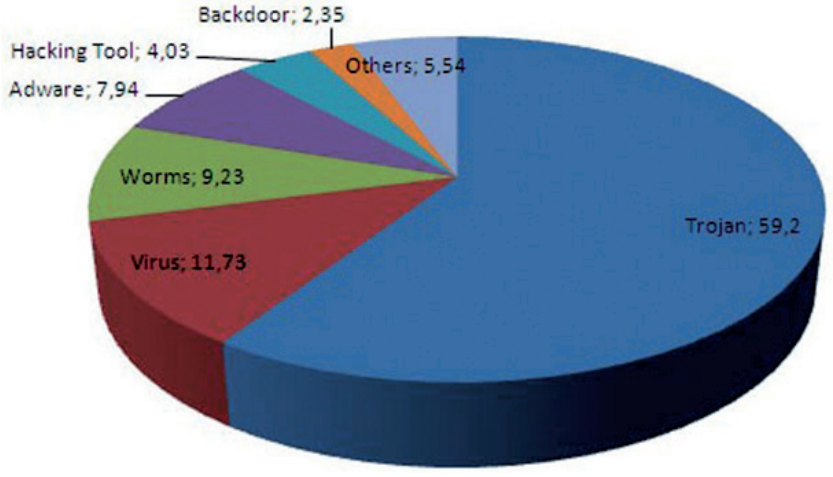
تنوع و پیچیدگی Exploit packها مبارزه با خطرات آنها را بسیار مشکل می‌کند. ارتش سایبری جمهوری اسلامی‌ایران تا کنون بسیاری از حملات خود را با Exploit packها انجام داده است؛ بسته‌های هکری که از بازار سیاه تولید Exploit خصوصا در روسیه خریداری شده‌اند. هیچ راه حل قطعی و دائمی برای مقابله کامل با Exploit packها وجود ندارد، چون اکسپلویت‌ها با ظهور آسیب‌پذیری‌های امنیتی جدید به سادگی به روز می‌شوند. در بازاری که با چند صد دلار می‌توان چنین بسته‌هایی را تهیه کرد، پرداخت میلیون‌ها دلار توسط دولت‌ها، چاره چندانی برای قربانیان باقی نمی‌گذارد، اما به هر حال اولا می‌توان سیستم خود را خالی از اطلاعات فوق‌العاده حساس نگاه داشت و ثانیا با اجرای تدابیر زیر، Exploitهای ابتدایی را از نفوذ بازداشت:

- نرم‌افزارها و خصوصا سیستم عامل خود را همواره آپدیت نگاه دارید. شرکت‌های بزرگ نرم‌افزاری جدیدترین Exploit packها را خریداری و فورا نرم‌افزارهای خود را با ارسال بسته‌های آپدیت و یا Patchهای امنیتی در برابر آن تهدیدها نفوذناپذیر می‌کنند.
- از Secure DNS مثلا شرکت Comodo استفاده کنید؛ بسیاری از شرکت‌های امنیت کامپیوتری، سایت‌های آلوده به ابزارهای Exploit را شناسایی می‌کنند؛ مثلا شرکت‌های سیمانتک، کاسپرسکی و مک‌آفی. فهرست سایت‌های آلوده سیمانتک نشان می‌دهد یک سایت آلوده به نام «Aladel.net» به تنهایی حاوی ۵۶۳۷۱ تهدید جدی علیه بازدیدکنندگان بوده است.
- از مرورگرهای آپدیت شده، خصوصا گوگل کروم استفاده کنید، کروم سایت‌های آلوده را شناسایی می‌کند و دیتابیس آن که به صورت روزانه آپدیت می‌شود، قبل از ورود شما به هر سایت مخرب به شما اخطار امنیتی به شکل زیر می‌دهد:

۳

بدافزارها[1]

بدافزارها مجموعه گسترده‌ای از نرم‌افزارهای آلوده و مخرب هستند که بدون اجازه شما، وارد سیستم شده و با اهداف متفاوتی موجب زیان، از بین رفتن داده‌ها و یا نرم‌افزارهای شما می‌شوند. در بخش‌های قبل، دورنمایی از وضعیت تهدیدهای اینترنتی ارائه شد. مطالعه نمودار زیر به دانشجویان کمک می‌کند تا سهم هر بدافزار از برنامه‌های مخرب نصب شده روی کامپیوترهای کاربران معمولی در سال ۲۰۱۰ را به صورت تقریبی مشاهده نمایند.



1. Malwares

نکاتی که می‌تواند برای دانشجویان جالب توجه باشد:

• همانطور که مشاهده می‌کنید تروجان‌ها یا اسب‌های تروا بخش اعظم بازار جهانی بدافزارها را قبضه کرده‌اند و این به این معناست که کاربران شخصی یا تجاری سطح متوسط یا پایین‌تر از آن، آسیب‌پذیرترین و پرتعدادترین قربانیان هستند.

• ویروس‌های کامپیوتری علی‌رغم سابقه چند دهه‌ای، قابلیت خودتکثیری و عنوانی ترسناک، تنها ۱۱/۷۳ درصد بدافزارها را نمایندگی می‌کنند.

پیشنهاد برای نحوه تدریس بدافزارها

برای ارائه تصویری نزدیک به واقع از خطرات بدافزارها، روش زیر پیشنهاد می‌شود:

• Virus یا ویروس: برنامه‌هایی که کامپیوتر شما و حتی دیگر کامپیوترهای سرور شما را آلوده می‌کنند و قابلیت خودتکثیری دارند. معمولا شما را فریب می‌دهند که مثلا ایمیلی را بازکنید، روی لینک خاصی کلیک کنید، فایلی را که دانلود کرده‌اید بازکنید و...

• Worm یا کرم: شما کار خاصی انجام نمی‌دهید، با استفاده از ضعف‌ها و حفره‌های امنیتی سیستم شما وارد دستگاه شما شده و در تمام شبکه پخش می‌شوند.

• Trojan یا اسب تروا یا تروجان: در ظاهری بی‌آزار، مثلا یک برنامه رایگان یا یک تصویر پس زمینه زیبا، وارد کامپیوتر شما می‌شوند، مدتی به انتظار می‌مانند و بعد درهای امنیتی کامپیوتر شما را به روی مهاجمان می‌گشایند.

• Rootkit یا روت‌کیت: بدون اطلاع شما مدیریت سیستم شما را در دست می‌گیرد، داده‌های شما را تخریب می‌کند و یا مانند باتنت‌ها، بخشی از منابع سیستم شما را در اختیار مهاجمان قرار می‌دهد.

• Scare-ware یا برنامه ترساننده: هنگام بازدید از اینترنت پنجره‌ای به شما می‌گوید سیستم شما آلوده شده و باید فلان برنامه را برای پاک کردن خطرات و یا افزایش سرعت کامپیوتر دانلود کنید.

• Spyware یا برنامه جاسوسی: بدون اطلاع شما مثلا تاریخچه سر زدن شما به سایت‌های مختلف را ضبط و برای سرور مرکزی خود ارسال می‌نمایند. این برنامه‌ها می‌توانند کلیدهایی که شما فشار می‌دهید را نیز ذخیره و ارسال کنند و از این طریق پسوردهای شما را به دست آورند.

• Botnet یا باتنت، بدون اطلاع شما و عموما از طریق آلوده شدن به یک تروجان یا روت‌کیت، کامپیوتر شما به «زامبی» یا عضوی از یک شبکه بزرگ تبهکاری تبدیل می‌شود. این شبکه برای مقاصد تبهکارانه یا جنگ سایبری علیه کشورها و سازمان‌های دیگر مورد استفاده قرار خواهد گرفت.

• Spam یا ایمیلی که شما مایل به دریافت آن نیستید: برای میلیون‌ها فرد ارسال می‌شوند عموما با موضوعاتی مثل پولدار شدن سریع، داروهای جنسی، زیبایی اندام و مواد آرایشی بسیار ارزان ارسال می‌شوند؛ این ایمیل‌ها معمولا حاوی لینک‌های آلوده هستند.

بدافزارهای را بر اساس پیشینه تاریخی می‌توان به گروه‌های مختلف زیر تقسیم کرد:

- تروجان یا اسب تروا (Trojan Horse)
- بمب منطقی (Logic Bomb)
- درب پشتی (Back Door)
- ویروس (Virus)
- کرم (Worm)
- خرگوش (Rabbit)
- جاسوس‌افزار (Spyware)
- تبلیغ‌افزار (Adware)
- بدافزار ترکیبی، قطره‌چکان، تهدید مخلوط (Hybrid, Dropper, Blended threat)
- زامبی (Zombie)

تروجان یا اسب تروا (Trojan Horse)

تروجان‌ها غالبا در شکل برنامه‌های سودمند توسط کاربران بر روی سیستم‌ها نصب می‌شوند. بلافاصله و یا پس از مدتی کد آلوده تروجان فعال می‌شود، برخی از فایل‌ها و یا تنظیمات شما را از بین می‌برد. در بسیاری از موارد تنظیم‌بندی‌های ایمنی کامپیوتر شما را هدف قرار می‌دهد و زمینه دسترسی تبهکاران به داده‌های شما را فراهم می‌آورد. استفاده از نرم‌افزارهای اشتراک داده‌هایی مثل فیلم و موزیک، همچنین استفاده از نرم‌افزارهای کرک (crack) شده و غیرقانونی از ساده‌ترین راه‌های نصب تروجان‌ها روی کامپیوتر شماست. بسیاری از این برنامه‌های مجانی کرک و یا قفل شکسته صرفاً به منظور ورود تبهکاران به کامپیوترهای شخصی قربانیان و سرقت اطلاعات، در سطح وسیعی منتشر می‌شوند.

یک نکته ساده اما کاربردی و مهم در تشخیص تروجان‌ها، توجه و دقت به فرمت فایلی است که از طریق مسنجرها یا ایمیل‌ها دریافت می‌کنید. اگر طرف مقابل شما ادعا می‌کند که در حال ارسال عکس است، اما فرمت فایل ارسالی EXE. (فرمت فایل‌های اجرایی و اپلیکیشن‌ها) است، تردید نکنید که باید از پذیرش و دریافت فایل خودداری کنید، چون حتما تروجان یا فایل مخرب دیگری بر اثر دریافت آن روی سیستم شما نصب خواهد شد.

با نگاهی به این اینفوگرافیک ساده اما پربار، می‌توانید اطلاعات جالبی درباره انواع تروجان‌ها و کارکردهای متفاوت آنها به دست آورید و در اختیار کارآموزان امنیت سایبری قرار دهید:

http://trojanwatch.org/wp-content/uploads/2011/11/trojans.png

بمب منطقی (Logic Bomb)

هر بمب منطقی، وقوع یک شرط یا گزاره منطقی را بر روی سیستم میزبان بررسی می‌کند، مثلا آیا امروز پنجشنبه ۲۴ ژوئن ۲۰۱۰ است یا نه؟ به مجرد تحقق این شرط بمب فعال می‌شود و به سیستم شما آسیب می‌رساند.

درب پشتی (Back Door)

این بدافزار با مکانیسمی نظیر بمب‌های منطقی، قطعه‌ای از برنامه‌ای به ظاهر سالم و پاکیزه است که در صورت وقوع شرط یا شروطی خاص، زمینه دسترسی مهاجمین به داده‌های شما را فراهم می‌آورد. مثال بسیار ساده به این شکل است: یک برنامه‌نویس می‌تواند برنامه‌ای برای امنیت کامپیوتر شما تولید کند که مانع ورود مهاجمان شود، اما او در داخل برنامه راهی برای ورود خود به کامپیوتر شما باز گذاشته و می‌تواند از آن در وارد سیستم شما شود.

ویروس (Virus)

ویروس‌ها از پایان دهه ۱۹۸۰ میلادی از عمده ترین خطرات و تهدیدها علیه امنیت سایبری به شماره می‌روند. ویروس‌ها را بر اساس مکانیسم تخریب و انتشار آنها می‌توان به گروه‌های متفاوتی تقسیم کرد، نظیر:

• ویروس‌های بوت‌سکتور یا ویروس‌هایی که سکتور صفر دیسک‌های حاوی اطلاعات را نشانه رفته، سعی در تکثیر از طریق آلوده کردن دیسک‌های دیگر دارند.

• ویروس‌های آلوده‌کننده فایل‌های اجرایی نظیر exe. ، com. و bin. که از طریق تغییر فایل‌های اجرایی سیستم و تکثیر در زیرشاخه‌ها و برنامه‌ها، داده‌های شما را تخریب و در انتظار انتقال به رایانه قربانی دیگری می‌نشینند.

• ویروس‌های ترکیبی که ترکیبی از عملکرد ویروس‌های بوت‌سکتور و ویروس‌های فایل‌های اجرایی دارند.

ویروس‌های زیر موجب وارد آمدن خسارات بسیار گزاف در سطح جهانی شدند:

Sircam 2001, Nimda 2001, Magistr 2001, Melissa 1999, Mydoom 2004, CIH Chernobyl 2001.

همزمان با تولید و انتشار ویروس‌ها، شرکت‌های امنیت کامپیوتری نیز نرم‌افزارهای ضدویروس بسیاری ارائه کرده‌اند. ویژگی مشترک همه این نرم‌افزارها، ضرورت به روزرسانی (Update) بانک اطلاعات ویروس‌های هر یک از آنها است. اگر کامپیوتر شما به شبکه اینترنت وصل باشد این عمل عموما به صورت اتوماتیک انجام می‌شود. اما همیشه از آپدیت بودن آنتی‌ویروس خود اطمینان حاصل کنید. آپدیت اتوماتیک از شروط لازم برای تأمین امنیت سیستم‌ها و شبکه‌ها است، اما شرط کافی نیست.

برای کاربرانی که به شبکه اینترنت متصل‌اند، امکان فراخوانی (Load) نرم‌افزارهای آنلاین ضدویروس وجود دارد به این صورت که با دانلود موتور جستجوی ویروس، نرم‌افزار ویروس‌یاب آنلاین، حافظه کامپیوتر شما را به دنبال ویروس‌ها جستجو می‌کند. در سال‌های گذشته شرکت‌های نرم افزاری معتبری، بسته‌های ویروس‌یاب و ویروس‌کش مجانی در اختیار کاربران کامپیوترهای شخصی قرارداده‌اند. بسته‌هایی که به سادگی از شبکه جهانی اینترنت قابل دانلود هستند. در بخش‌های بعدی در خصوص نحوه مقابله با ویروس‌ها و نصب و استفاده از ضدویروس‌ها بیشتر صحبت خواهیم کرد.

در این اینفوگرافیک می‌توانید با ۲۵ ویروس مشهور جهان دیجیتال آشنا شوید و توضیحات مختصری

درباره آنها بخوانید. در صورتی که می‌خواهید اطلاعات عمیق‌تر و دقیق‌تری از تاریخچه آنها و نحوه کارکردشان داشته باشید، کلیدواژه‌های موجود در این اینفوگرافیک راهنمای بسیار مناسبی خواهد بود.

http://hackingtools.co.in/25-most-famous-computer-viruses-infographic/

همچنین این مجموعه عکس در مجله «پاپیولار ساینس» نیز اطلاعات جالبی درباره ۱۰ ویروس شناخته‌شده در تاریخ تکنولوژی‌های دیجیتال ارائه کرده است:

http://www.popsci.com/scitech/gallery/2009-04/top-10-computer-viruses

کرم (Worm)

تفاوت عمده کرم‌ها با ویروس‌ها به انتشار اتوماتیک و خودکار کرم‌ها باز می‌گردد. کرم‌ها با شناسایی حفره‌های امنیتی یک سیستم عامل، یک شبکه و یا یک پروتکل انتقال داده معین، خود را تکثیر و وارد کامپیوتر شخصی شما می‌کنند.

برخی از مخرب‌ترین کرم‌های کامپیوتری که سرورها و شبکه‌های کامپیوتری را با اختلالات جدی مواجه کردند عبارتند از:

Anna Kournikova worm 2001, Klez worm 2001, Explorer worm 1999, Bad Benjamin worm 2002, Loveletter worm 2000, Sasser worm 2004, Blaster worm 2003, Sobig worm 2003.

یکی از مهم‌ترین کرم‌های کامپیوتری سال‌های اخیر، استاکس‌نت است که برای بمباران مجازی تأسیسات هسته‌ای ایران مورد استفاده قرار گرفت. برای کسب اطلاعات بیشتر درباره این کد مخرب که برنامه‌ای ۱۵ هزار خطی در پس آن است، اینجا را بخوانید:

http://www.dw.de/dw/article/0,,15343414,00.html

این ویدئوی ۳ دقیقه‌ای هم آناتومی استاکس‌نت، این اسلحه سایبری ویرانگر را نشان می‌دهد:

http://youtu.be/scNkLWV7jSw

برای درک دقیق‌تر تفاوت‌های موجود میان ویروس‌ها، کرم‌ها و تروجان‌ها و نیز راهکارهای مقابله با آنها این مقاله را بخوانید:

http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp

خرگوش (Rabbit)

این بدافزارها برنامه‌هایی کمیاب هستند که مانند خرگوش و یا باکتری با سرعت بسیار زیادی خود را تکثیر می‌کنند. بسیاری از آنان با افزایش سریع، تمام منابع سیستم شما را به خود اختصاص داده و عملا کامپیوتر شما را فلج می‌کنند. نمونه ساده آن قطعه برنامه‌ای است که در هر ثانیه چند پنجره جدید می‌گشاید. این عمل بسیاری از توان سی.پی.یو و حافظه شما را به خود اختصاص داده و کامپیوتر را عملا قفل می‌کند.

حالت دیگر خرگوش‌ها برنامه‌ای است که بلافاصله پس از تولد، مادر خود را پاک می‌کند. مثلا در

شکلی از یک کرم که میان کامپیوترهای مختلف شبکه در حال جست و خیز است و هر بار قطعه و یا برنامه مولد خود را پاک کرده با شکل جدیدی در کامپیوتری دیگر ظاهر می‌شود.

جاسوس‌افزار (Spyware)

برنامه‌های جاسوس، پس از ورود و استقرار بر روی سیستم شما، سعی در جمع‌آوری اطلاعات غیرمجاز و ارسال آن برای فرستندگان خود دارند؛ مثلا شناسه‌ها و یا رمزهای ورود، آدرس ایمیل دوستان شما و یا مشخصات مالی، فایل‌های متن و غیره. بسیاری از صفحات اینترنتی به محض باز شدن و مرور، برنامه‌های جاسوس را به حافظه کامپیوتر شما منتقل می‌کنند. تفاوت اساسی برنامه‌های جاسوس و ویروس‌ها یا کرم‌ها، عدم توانایی برنامه‌های جاسوس در تکثیر کردن خود و یا انتقال به کامپیوترهای مختلف است. یکی از متداول‌ترین و رایج‌ترین برنامه‌های جاسوس کامپیوتری، برنامه‌های ضبط‌کننده صفحه کلید یا Keyloggerها هستند، این برنامه‌ها هر کلیدی را که روی صفحه کلید شما فشرده شود ضبط کرده و سپس همه این مجموعه را برای دریافت‌کننده اطلاعات جاسوسی ارسال می‌دارند. این کلیدها می‌تواند مجموعه کامل گفتگوی چت نوشتاری شما، رمزهای ورود به ایمیل و یا نگارش متن یک گزارش و یا ایمیل بر روی کامپیوتر شما باشد. برنامه‌های جاسوس دیگری برای جاسوسی از وب‌کم شما، میکروفن لپ‌تاپ و یا ضبط صفحه نمایش وجود دارند. به این معنی که پس از فعال شدن، همه رویدادهای صفحه نمایش شما را ضبط و به مرور به خارج از کامپیوتر شما قاچاق می‌کنند.

از اینجا می‌توانید اطلاعات آماری جالب و مختصری درباره جاسوس‌افزارها ببینید:

http://www.infospyware.net/blog/where-does-your-malware-come-from/

تبلیغ افزار (Adware)

همه شما برنامه‌های آگهی را تجربه کرده‌اید، برنامه‌هایی که با بازکردن صفحات خاص یا ظاهر کردن بنرهای متعددی، شما را به خرید محصولات و یا استفاده از سرویس‌های خود توصیه می‌کنند. برنامه‌های تبلیغی نیز مانند Spywareها فاقد توان تکثیر خود هستند. این برنامه‌ها می‌توانند داده‌های شما را دستخوش تغییر کنند و در برخی موارد تنظیمات کامپیوتر شما را تغییر دهند. مثلا صفحه جستجوی پیش فرض شما را به سایت خود تغییر داده و یا به هنگام جستجوی محصولات برای خرید، شما را به صورت خودکار به محصولات مورد نظر خویش، هدایت نمایند.

بدافزار ترکیبی، قطره‌چکان، تهدید مخلوط (Hybrid, Dropper, Blended threat)

هیبریدها به ترکیبی از تهدیدهای ذکر شده در موارد قبل اطلاق می‌شود؛ برنامهٔ جاسوسی که در عین حال یک اسب تروا و یا یک ویروس را نیز در کامپیوتر قربانی نصب می‌کند یا به طور مثال قطعه برنامه‌ای که اولا یک «درب پشتی» ایجاد کرده و ثانیا این عمل را شبیه یک ویروس بر فایل‌های دیگر آن سیستم تکرار می‌کند.

قطره‌چکان‌ها یا Dropperها نیز می‌توانند با روش‌های ترکیبی، حفره‌هایی در کامپیوتر قربانی از خود بر جای گذارند، مثلا ویروسی که علاوه بر بازنشر خود، یک «درب پشتی» هم روی کامپیوتر میزبان بر جای می‌گذارد.

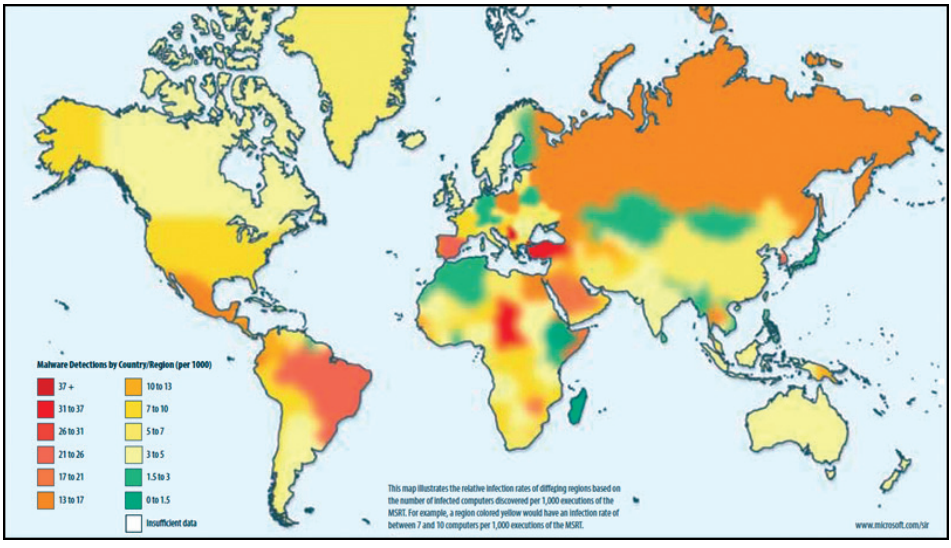
تهدید مخلوط یا Blanded Threat به ویروسی اطلاق می‌شود که از روشی مشابه کرم‌ها برای کشف آسیب‌پذیری‌های تکنیکی شبکه یا پروتکل استفاده کرده و در عین حال بر خلاف کرم توان تکثیر دارد.

زامبی (Zombie)

بسیاری از بدافزارها مثلا اسب‌های تروا پس از در اختیار گرفتن کامپیوتر قربانی، از آن برای مقاصد غیرقانونی خود استفاده می‌کنند. این مقاصد می‌تواند ارسال هرزنامه (Spam) و یا حملاتی چون حمله توزیع شده به منظور توقف سرویس (distributed denial-of-service attack - DDoS attack) باشد. در این مرحله قربانی بدون آنکه خود بداند بخشی از شبکه بزرگ حمله و اقدامات غیرقانونی تبهکاران است. به طور مثال در جریان حملات گسترده سایبری علیه دولت استونی در سال ۲۰۰۷، سازمان‌دهندگان حملات از شبکه‌های بات‌نت و کامپیوترهای زامبی ارسال‌کننده هرزنامه برای اجرای یک حمله بزرگ DDoS استفاده کردند.

تولید و توسعه بدافزارها، تجارت بزرگی در دنیای امروز است که هر ساله میلیون‌ها دلار گردش مالی دارد. در این اینفوگرافیک اطلاعات جالبی درباره این موضوع آمده است:

http://www.axleration.com/inside-the-malware-business-infographic/



تاریخچه بدافزارها

برای آشنایی دانشجویان با تاریخچه عمده‌ترین بدافزارها می‌توان از جدول زیر استفاده کرد:

اولین ویروس برای کامپیوترهای شخصی	پاکستان	1986	Brain
توسط یک دانش‌آموز دبیرستانی نوشته شد	نیوزلند	1987	Stoned
یکی از بزرگترین موارد پخش ویروس در سراسر جهان	سوئیس	1990	Form
نخستین ویروس کامپیوتری که وارد ادبیات رسانه‌ای شد	نیوزلند	1991	Michelangelo
تولد اتوماتیک ویروس با یک ظاهر ساده گرافیکی	آمریکا	1992	VCL
برنامه با قابلیت مخفی‌سازی خودکار	کانادا	1994	Monkey
اولین ویروسی که فایل‌های مایکروسافت وُرد را آلوده کرد	آمریکا	1995	Concept
اولین ویروس ایمیلی	نامشخص	1999	Happy99
ظاهرا ملیسا نام یک رقصنده است	آمریکا	1999	Melissa
شیوع اولین کرم بدون هیچ نوع دخالت کاربر	نامشخص	2001	Code Red
با attachment ایمیل، یکی از بزرگترین موارد شیوع و تخریب	فیلیپین	2000	Love Letter
خودپردازهای Bank of America و 911 سیاتل را از کار انداخت	نامشخص	2003	Slammer
در کمتر از چند ساعت، میلیون‌ها کامپیوتر را آلوده کرد	نامشخص	2003	Sobig
اولین ویروس با هدف کسب درآمد با ارسال اسپم	نامشخص	2003	Fizzer
اولین کرم روی تلفن‌های موبایل	فیلیپین	2003	Cabir
تکثیر از طریق ایمیل و شبکه‌های محبوب p2p، مشخصا Kazaa	روسیه	2004	MyDoom
شبکه‌ها را از استرالیا تا هنگ‌کنگ و انگلستان از کار انداخت	آلمان	2004	Sasser
اولین تروجان با قابلیت عبور از ضدویروس‌های معمولی	نامشخص	2004	SdBOT
روت‌کیت برای ویندوز با قابلیت اختفای بدافزارهای دیگر	نامشخص	2005	Haxdoor
روت‌کیت که توسط SONY BMG نصب می‌شد	آمریکا، انگلیس	2006	Sony Rootkit
قابلیت سرقت اطلاعات حساس مثل حساب بانکی	نامشخص	2007	Mebroot

پیامی را درباره تلفات طوفان در اروپا نمایش می‌داد	نامشخص	2007	StormWorm
موبایل‌های مبتنی بر سیستم عامل ویندوز را آلوده می‌کرد	روسیه	نامشخص	3D-Anti Terrorist
به سرعت، میلیون‌ها کامپیوتر در سراسر جهان را آلوده کرد	نامشخص	2008	Conficker
با حجمی‌حدود ۱۰۰۰ برابر یک کرم معمولی	آمریکا، اسرائیل	2010	Stuxnet

برای اطلاع بیشتر از هر یک از این ویروس‌ها، می‌توانید نام آن را در کتابخانه شرکت‌های بزرگ ضدویروس نظیر سیمانتک جستجو کنید. مثلا برای ویروس استاکس‌نت:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

۴

امنیت کامپیوتر و وب

راهنمای آموزش امنیت پسورد و حساب کاربری

شیوه‌های حدس پسورد با روش موسوم به دیکشنری را به دانشجویان توضیح دهید و از آنان بخواهید چند پسورد مختلف مثلا Tehran1234، Shiva1363، Ty@N14_B، MyPassword را با یکدیگر مقایسه کنند.

• چند کاربر به کامپیوتر شما دسترسی دارند؟ بهترین حالت، دسترسی یک کاربر یعنی شما، با حق دسترسی ادمین است. کاربرهای میهمان امنیت کامپیوتر شما را پایین می‌آورند.

• اکثریت قریب به اتفاق کاربران کامپیوترهای شخصی از یک پسورد واحد برای ورود به کامپیوتر، ایمیل، اسکایپ و حتی بانک آنلاین خود استفاده می‌کنند. برای دانشجویان توضیح دهید که چرا این روش به شدت خطر آفرین است.

• استفاده و تایپ پسورد در کافی‌نت‌ها یا کامپیوتری که متعلق به شما نیست، درست مانند فریاد کردن پسورد خود در کوچه و خیابان است. حتی الامکان در چنین مواردی اولا از حالت ناشناس مرورگرها استفاده کنید و ثانیا از اکانت‌های خود کاملا Log out کرده، فایل‌های کمکی اینترنت را با دقت پاک کنید.

مثال: امنیت جی‌میل

شرکت گوگل با ارائه جی‌میل امکانات مناسبی برای تبادل ایمیل فراهم آورده است. نگارنده استفاده از جی‌میل را به دلایل فنی بسیار توصیه می‌کند. جی‌میل نیز مانند هر سرویس‌دهنده ایمیل دیگر صد درصد امن نیست، بنابراین بهتر است چند ایمیل مختلف داشته باشید و بسته به طبقه‌بندی و میزان اعتماد خود به افراد، ایمیل متناسب با آن سطح را در اختیار آنان قرار دهید:

Amir_Tafreshi@gmail.com برای کارهای اداری، دانشگاه و افراد ناشناس و مطالب عمومی

Amir.Tafreshi@gmail.com برای خانواده، دوستان و مطالب خصوصی با اهمیت متوسط

Amr_Trfs@gmail.com برای دوستان فوق‌العاده نزدیک، مطالب فوق‌العاده حساس و خصوصی

ایران کشور مناسب یادگاری نگاه داشتن نیست؛ ایمیل حاوی مطالب حساس را بلافاصله پس از مطالعه پاک کنید و دقت کنید که از Trash نیز پاک شده باشند. امنیت شوخی‌بردار نیست؛ ارسال تصاویر میهمانی خصوصی و از آن حساس‌تر تصاویر خلوت (intimate) افراد در ایران به طور بالقوه به خطر انداختن تحصیل، شغل و حتی جان آنها است.

توصیه‌های عمومی مربوط به پسورد را در مورد پسورد ایمیل خود جدی بگیرید. شرکت گوگل اخیرا سرویس دو مرحله‌ای پسورد خود (2 step verification) را برای کاربران ایرانی فعال کرده است. این تدبیر متعاقب حملات سازماندهی شده توسط دولت ایران علیه کاربران ایرانی گوگل انجام پذیرفت.

به دانشجویان توصیه کنید از وبلاگ رسمی گوگل به زبان فارسی و همچنین بخش امنیت سایبری رادیو فردا مرتبا بازدید به عمل آورند:

http://googlepersianblog.blogspot.com/

http://www.radiofarda.com/content/f7_commentary_over_making_gmail_more_secure/24324496.html

دو توصیه بسیار جدی در خصوص جی‌میل

۱. به دانشجویان بیاموزید که به هیچ وجه attachment از افراد ناشناس باز نکنند. متأسفانه بسیاری از attachmentها به نام افراد آشنا ارسال می‌شود، بنابراین بهتر است از باز کردن فایل‌های attachment روی کامپیوتر حساس خودداری نمائید.

۲. کنار آدرس سایت جی‌میل، مانند تصویر زیر همواره می‌بایستی به رنگ سبز باشد، امنیت گواهینامه‌های SSL را جدی بگیرید:

جزییات بیشتر درباره پسوردهای دومرحله‌ای که تا حدود زیادی امکان جلوگیری از هک شدن و بازپس‌گیری اکانت جی‌میل در صورت هک شدن را فراهم می‌کند، از اینجا بخوانید (به فارسی):
http://www.dw.de/dw/article/0,,15359369,00.html

پست وبلاگ گوگل به زبان فارسی درباره فعال شدن پسوردهای دومرحله‌ای برای کاربران ایرانی:
http://googlepersianblog.blogspot.com/2011/12/blog-post.html

مشاهده ویدئوی گوگل درباره پسوردهای دومرحله‌ای به همه کاربران جی‌میل توصیه می‌شود:
http://www.youtube.com/embed/GtcVjOWHg9E?cc_load_policy=1&cc_lang_pref=fa

چند نکته امنیتی مهم درباره جی‌میل در وبلاگ رسمی گوگل به زبان فارسی:
http://googlepersianblog.blogspot.com/2012/01/gmail.html

فراموش نکنید که برای افزایش امنیت، همواره از HTTPS برای اتصال به جی‌میل استفاده کنید. فعال کردن آن بسیار ساده است.

بیشتر کاربران بی‌دقتی‌های فاحشی در انتخاب پسوردهای اکانت‌های گوناگون خود دارند. نگاهی به این اینفوگرافیک می‌تواند نکات مهمی را به کاربران ارائه کند تا پسوردهای امن‌تری انتخاب کنند:

اگر می‌خواهید جزئیات بیشتری درباره انتخاب پسوردهای محکم و امن بدانید، مطالعه این بخش مفصل در وب‌سایت لایف‌هکر توصیه می‌شود:

http://lifehacker.com/5876541/use-this-infographic-to-pick-a-good-strong-password

این مطلب اطلاعات جالبی درباره ضعیف‌ترین و پرکاربردترین پسوردهای کاربران اینترنت ارائه کرده است:

https://www.azadcyber.info/articles/2429

اگر می‌خواهید اشتباهات فاحش عموم کاربران در انتخاب پسوردها و راه‌های مقابله با آنها را ببینید، این اینفوگرافیک را مشاهده کنید:

http://protectme.webroot.com/wp-content/themes/webroot/images/password-infographic.png

افزایش امنیت ایمیل‌ها با کدگذاری ارتباطات ایمیلی در Thunderbird

اگر از اکانت ایمیل خود (صرف‌نظر از اینکه از چه سرویسی استفاده می‌کنید؛ اعم از جی‌میل، یاهو، هات‌میل و...) برای انتقال داده‌های حساس و محرمانه استفاده می‌کنید، می‌توانید برای افزایش امنیت از نرم‌افزار مدیریت ایمیل‌های کمپانی موزیلا، موسوم به Thunderbird استفاده کنید. با فعال کردن کدگذاری PGP در Thunderbird، تنها طرفین تماس با استفاده از کدهایی که پیش‌تر بر سر آن توافق کرده‌اند، می‌توانند محتوای محرمانه را رمزگشایی و مشاهده کنند. الگوریتم کدگذاری این سیستم به‌گونه‌ای است که می‌توان گفت رمزگشایی آن برای مهاجمان یا نیروهای کنترل‌گر تقریبا ناممکن است. برای پی‌گیری جزئیات این سیستم و نحوه نصب و راه‌اندازی آن، می‌توانید به اینجا مراجعه کنید:

http://lifehacker.com/180878/how-to-encrypt-your-email

در اینجا اطلاعات مفیدی در این باره خواهید یافت. اگر توصیه‌ها را گام به گام اجرا کنید، امنیت ایمیل و ارتباطات ایمیلی شما به طور محسوسی افزایش خواهد یافت.

https://security.ngoinabox.org/en/thuderbird_encryption

استفاده از نرم‌افزارهای مدیریت پسوردها برای افزایش امنیت

پیش‌تر اشاره کردیم که استفاده از پسوردهای یکسان از جمله اشتباهات رایج در میان کاربران اینترنت در سراسر جهان است که بر ضریب آسیب‌پذیری کاربران می‌افزاید. برای تسهیل استفاده از پسوردهای گوناگون برای سرویس‌های مختلف (که همیشه با معضل فراموشی کاربران مواجه است) می‌توانید از برنامه‌های مدیریت پسورد استفاده کنید.

KeePass یکی از این نرم‌افزارهاست. اطلاعات مرتبط با آن را از اینجا بخوانید:

http://keepass.info/

بسیاری از نرم‌افزارهای مدیریت پسورد، اپلیکیشن‌هایی برای موبایل و تبلت هم ارائه می‌کنند و به همین خاطر استفاده از آنها بسیار ساده است و همه جا می‌توانید به پسوردهای خود دسترسی داشته باشید

یا در صورت لزوم برای اکانت خود پسورد جدیدی تولید کنید.

از اینجا می‌توانید اطلاعات بیشتری درباره ۵ برنامه پرکاربرد مدیریت پسورد کسب کنید:

http://lifehacker.com/5042616/five-best-password-managers

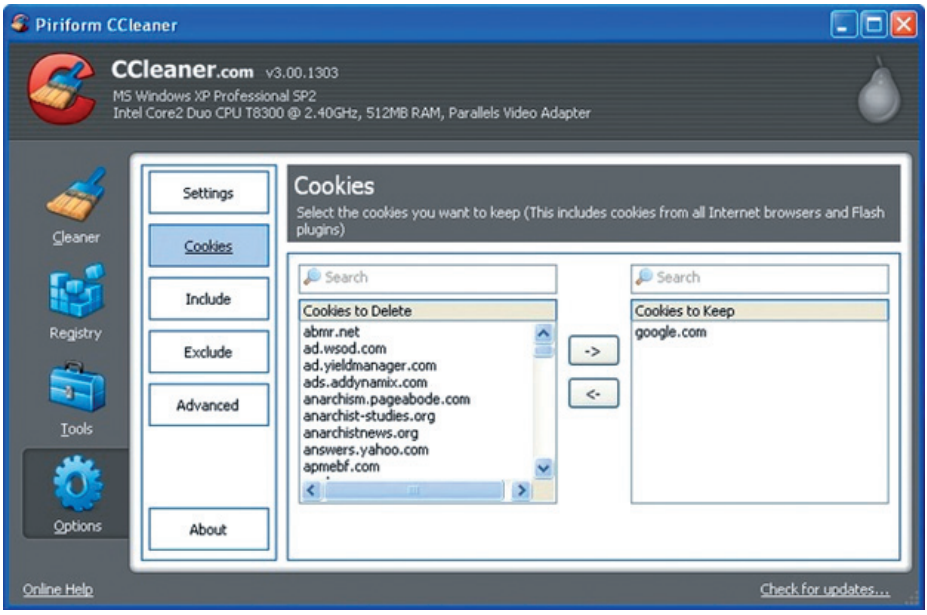
مثال: امنیت داده‌ها با CCleaner

در ایران چاره‌ای جز کدگذاری داده‌های حساس نیست. در انتهای این بخش، نرم‌افزار کارایی برای کدگذاری داده‌ها معرفی می‌شود.

یک مثال ساده می‌تواند دانشجویان را برای فهم امنیت داده‌ها یاری کند:

- یک کول دیسک USB را انتخاب کنید. سه عکس و یک فایل موسیقی mp3 را روی آن کپی کنید. از دانشجویان بخواهید که این سه فایل را پاک کنند. سپس با نرم‌افزاری مثل Recuva فایل‌های پاک شده را بازیافت کنید و به دانشجویان نشان دهید.

ما برای پاک کردن دائمی داده‌ها، نرم‌افزار قدرتمند، سریع و رایگان CCleaner از شرکت Trendmicro را پیشنهاد می‌کنیم:

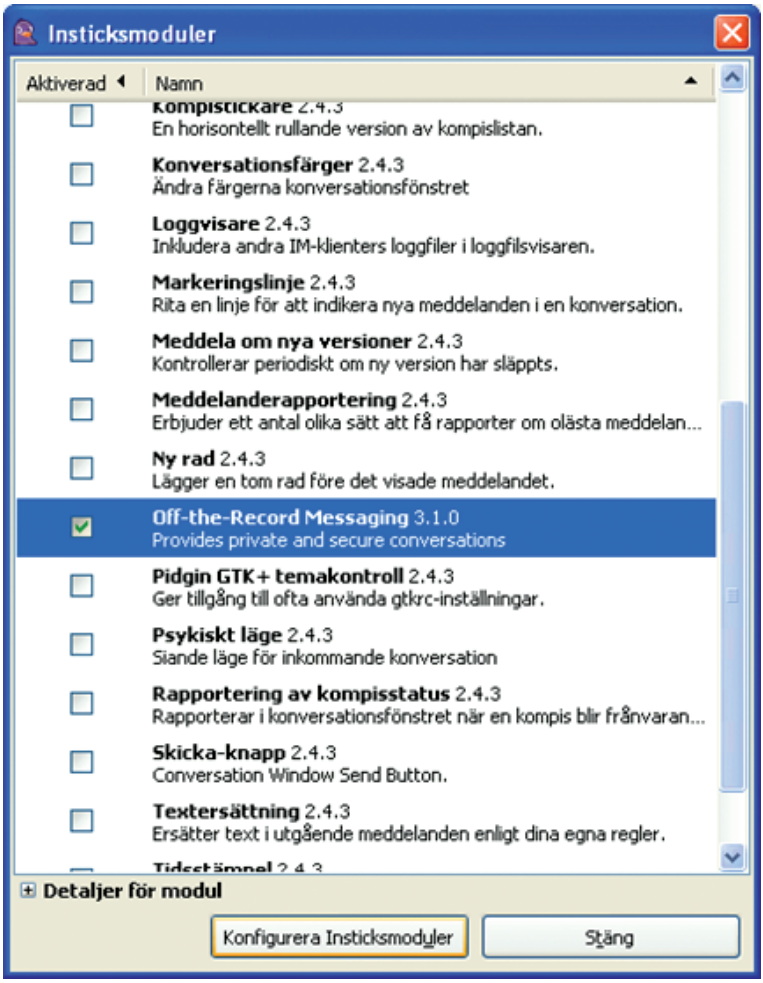


این نرم‌افزار قادر است، فایل‌های کمکی مرورگرهای شما را پاک کند و فایل‌های پاک شده شما را نیز برای همیشه غیرقابل بازیافت نماید. این نرم‌افزار همچنین توان پاک کردن داده‌های اضافی در رجیستری و همچنین استارت‌آپ کامپیوترهای ویندوز را نیز دارد.

مثال: امنیت مسنجرها با Pidgin

تقریبا هرکس که تجربه کار با یاهو مسنجر را داشته باشد، آلوده و هک شدن از طریق مسنجرها را تجربه کرده است. هکرها دهها و صدها ترفند متفاوت را برای نفوذ به کامپیوترها از طریق مسنجرها به کار می گیرند.

علاوه بر این شرایط ویژه ایران لزوم چت در حالت SSL را موجب شده است. ما برای ارتقای امنیت مبادلات متنی نرم‌افزار Pidgin در حالت OTR را پیشنهاد می کنیم:



این پلاگین برای پیدجین در آدرس زیر قابل دانلود است، مستندات نصب و استفاده از پلاگین نیز توسط تهیه‌کنندگان پلاگین ارائه شده است:

http://www.cypherpunks.ca/otr/

برای نصب نرم‌افزار اصلی پیدجین می‌توانید از لینک زیر استفاده کنید:

http://pidgin.im/download/

نکات عمومی‌حفظ امنیت در مسنجرها قبلا توضیح داده شده است، مسنجرها اساسا یکی از دروازه‌های عملیات مهندسی اجتماعی است، روی لینک‌هایی که در مسنجرها دریافت می‌کنید کلیک نکنید و اساسا از چت کردن با افرادی که نمی‌شناسید حتی الامکان خودداری کنید.

با تنظیم پیدجین می‌توانید چت خود را در سرویس‌های مختلف (جی‌میل، یاهو و...) به‌گونه‌ای مدیریت کنید که محتوای گفت‌وگوها کاملا محرمانه بماند. پیدجین برای «احراز هویت» طرف گفت‌وگو هم امکانات جالب و کم‌نظیری به کاربران ارائه می‌کند که همه آنها در راستای افزایش امنیت و تضمین محرمانگی داده‌ها طراحی و پیاده‌سازی شده‌اند.

وب‌سایت لایف‌هکر، اطلاعات جالب و کاربردی و مفیدی درباره نرم‌افزار محبوب پیدجین ارائه کرده است که از اینجا قابل دسترسی است:

http://lifehacker.com/356291/ten-must+have-plug+ins-to-power-up-pidgin

امنیت مرورگرها (Browsers)

آخرین نسخه‌های اینترنت اکسپلورر، فایرفاکس، گوگل کروم و اپل سافاری و همچنین اپرا، از قابلیت بلوک کردن و محافظت کامپیوتر شما در برابر سایت‌های حاوی نرم‌افزارهای آلوده و بدافزارها (malware) برخوردارند.

استفاده از آخرین نسخه مرورگر کروم به کاربران اینترنت در ایران توصیه می‌شود.

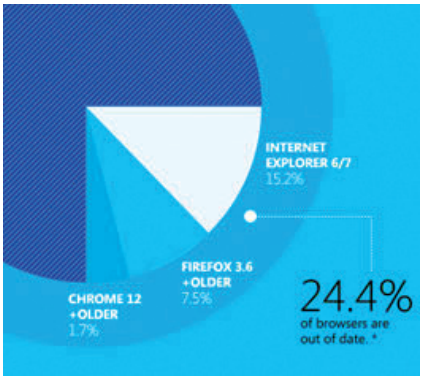
امکانات امنیتی کروم:

۱. مرورگری امن

- تشخیص سایت‌های حاوی malware با نمایش پیام Warning: Something's Not Right Here!
- تشخیص سایت‌های phishing با نمایش پیام Warning: Suspected phishing site!

۲. Sandboxing

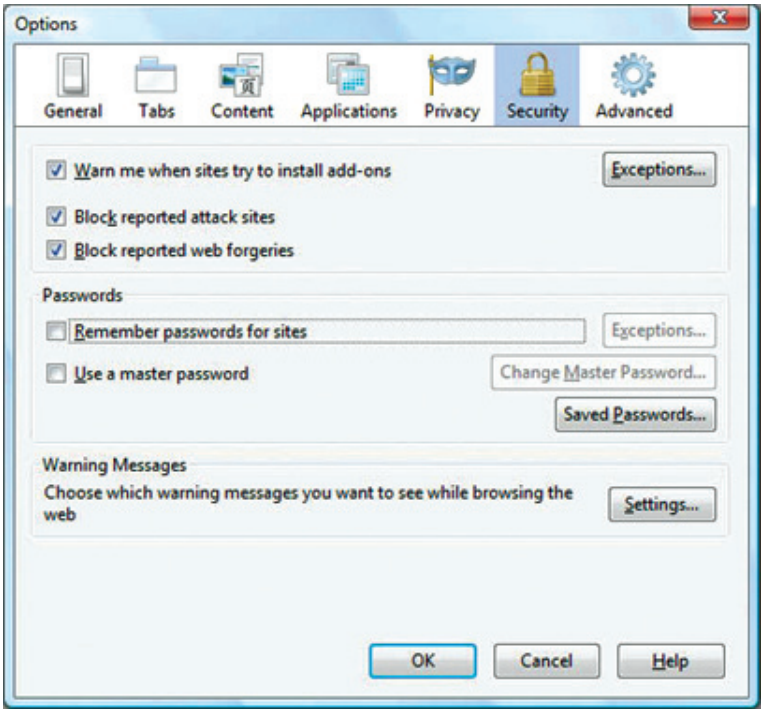
برای مقابله با خطر حملات موسوم به XSS، گوگل کروم پنجره‌های مختلف مرورگر را مستقل از یکدیگر مدیریت می‌کند تا مهاجمان نتوانند مثلا از پنجره یا Tab جدیدی که برای مشاهده یک عکس باز کرده‌اید، کوکی‌های ایمیل شما را که در پنجره یا Tab دیگری باز است دستکاری کنند. Sandboxing لایه جدیدی از امنیت را برای مقابله با سایت‌های حاوی بدافزار که کدهای آلوده‌ای را به حافظه کامپیوتر شما منتقل می‌کنند، ارائه نموده است.

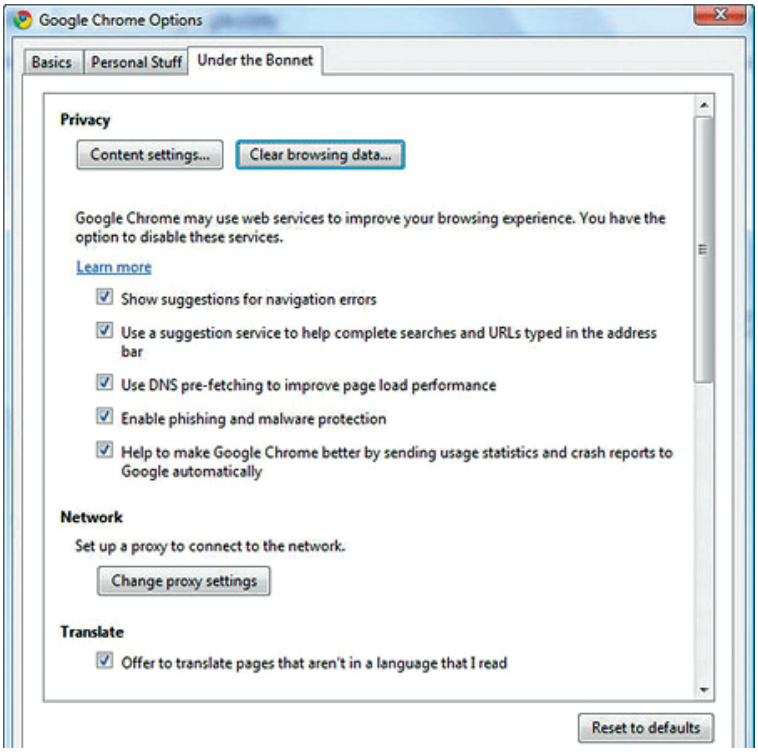


۳. Auto Update

بارها گفته شده است که مرورگرهای به روز نشده، تهدید جدی علیه امنیت کامپیوتر شما هستند. گوگل کروم از امکان آپدیت اتوماتیک برخوردار است.

فایرفاکس از امکان پیش ساخته‌ای برای تشخیص و مقابله با سایت‌های فیشینگ (Anti Phishing) استفاده می‌نماید که به گفته موزیلا، هر روز ۴۸ بار آپدیت می‌شود. همچنین سرویس مرور امن گوگل یا google safe browsing در فایرفاکس گنجانده شده است. این سرویس گوگل بر پایه شناسایی سایت‌های آلوده به بدافزارها و کدهای مضر استوار است. برای استفاده از سرویس‌های فوق می‌بایستی هر دو سرویس را به شکل زیر فعال نمایید. گوگل کروم نیز امکان کاملا مشابهی را عرضه نموده است که می‌توانید در قسمت مشابه تنظیمات کروم در صفحه بعد مشاهده نمائید:





اینترنت اکسپلورر در مقابل از تکنولوژی‌ای به نام SmartScreen technology استفاده می کند، شایان توجه است که این تکنولوژی در نسخه ۹ اینترنت اکسپلورر روی سیستم‌عامل‌های Win. Vista و Win. 7 قابل دسترسی است. تکنولوژی مورد ادعای مایکروسافت قادر است آدرس URL وب‌سایت‌های آلوده، سایت‌های حاوی نرم‌افزارهای آلوده، سایت‌های click-jacking و از همه مهم‌تر سایت‌های حاوی cross-site scripting (شیوه مورد استفاده ارتش سایبری سپاه برای هک سایت‌های بالاترین، زمانه و غیره) را بلوکه کند. این مرورگر همچنین برای جلوگیری از فیشینگ، آدرس واقعی صفحه را در قسمت بالا، به صورت برجسته نمایش می‌دهد تا کاربر به صورت لحظه‌ای در جریان تغییر آدرس صفحه باشند.

همچنین در این نسخه، امکان automatic crash recovery نیز گنجانده شده است. مایکروسافت راهنمای امکانات امنیتی اینترنت اکسپلورر ۹ را منتشر نموده است که در آدرس زیر قابل دسترسی و مطالعه است:

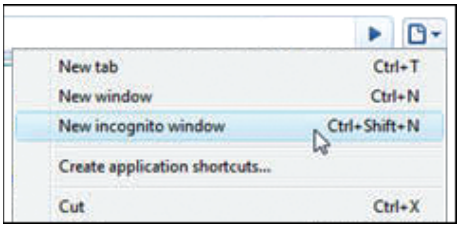
http://www.microsoft.com/en-gb/security/pc-security/ie9.aspx

اینترنت اکسپلورر ۹، فایرفاکس، سافاری و کروم هر چهار مرورگر قابلیت مرور صفحات و وبگردی با محافظت از مشخصات خصوصی کاربران را دارند. در این حالت، اولا کوکی‌ها اجراء نشده و بسیاری از مشخصات خصوصی کاربران محفوظ می‌ماند و ثانیا اجزای صفحات وب، تصاویر، آدرس‌ها و ویدئوها، در قسمت حافظه موقت یا cache ذخیره نخواهد شد. البته بایستی توجه داشت بسیاری از صفحات وب در این حالت برای اجراء با مشکل مواجه خواهند شد. مثلا دسترسی کاربران به صفحه Gmail محدود خواهد شد، به همین دلیل می‌توانید برخی از صفحات خود را از حالت خصوصی مستثنی کنید.

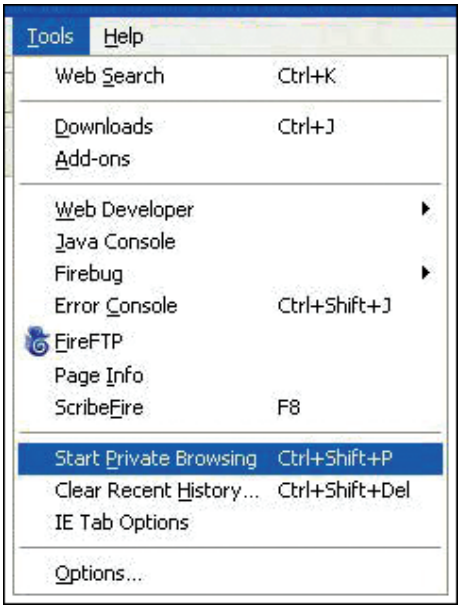
مرورگرهای مختلف از واژه‌های متفاوتی برای نامیدن حالت خصوصی خود استفاده نموده‌اند؛ این واژه‌ها به قرار زیر هستند:

- Internet Explorer → InPrivate
- Mozilla Firefox → Private Browsing
- Google Chrome → Incognito
- Safari → Private Browsing

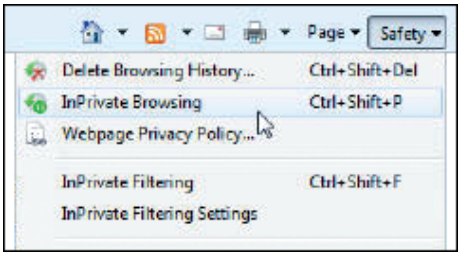
در مورد اجرای افزونه‌های مرورگرها مانند Silverlight و Flash، برخی از این افزونه‌ها و نرم‌افزارها سابقا قادر به ذخیره اطلاعات خصوصی کاربران در حافظه موقت بوده‌اند، اما به طور مثال شرکت Adobe، نرم‌افزار فلش ۱۰ را سازگار با حالت خصوصی یا Privacy mode در اینترنت اکسپلورر، فایرفاکس، کروم و سافاری عرضه نموده است.



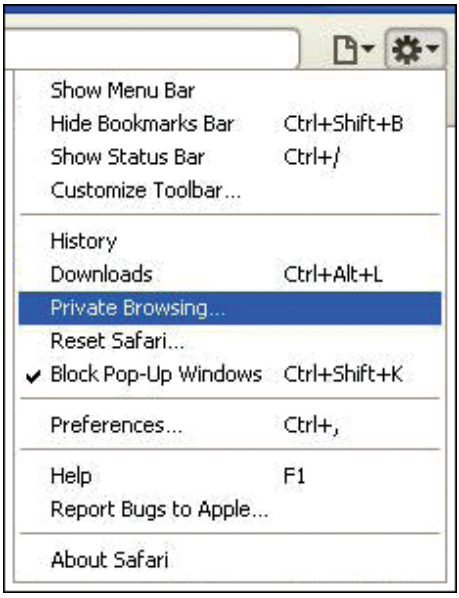
فعال کردن حالت خصوصی در کروم



فعال کردن حالت خصوصی در فایرفاکس



فعال کردن حالت خصوصی در اینترنت اکسپلورر



فعال کردن حالت خصوصی در سافاری

افزایش امنیت در فایرفاکس با افزونه HTTPS Everywhere

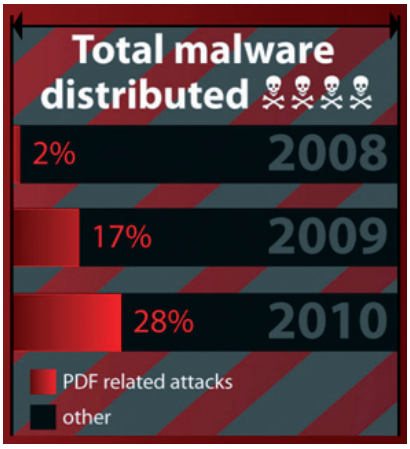
یکی از راه‌های حصول اطمینان از امنیت ارتباطات، استفاده از نسخه HTTPS وب‌سایت‌ها و سرویس‌ها است. با HTTPS فرایند تبادل اطلاعات میان کاربر و یک وب‌سایت یا سرویس آنلاین، محرمانه باقی می‌ماند و چون روی این پروتکل امن، مرورگر کاربر دائما در حال تایید هویت و چک کردن وضعیت وب‌سرور است، راهی برای نفوذ هکرها و قرار گرفتن آنها در میانه مسیر ارتباطی باقی نمی‌ماند.

اما همه کاربران حوصله و توان فعال کردن HTTPS برای سرویس‌های گوناگون را ندارند. کاربرانی که از مرورگر فایرفاکس برای وب‌گردی استفاده می‌کنند، با نصب افزونه HTTPS Everywhere که از محصولات بنیاد EFF است می‌توانند مطمئن شوند که اگر سایتی نسخه HTTPS دارد، مرورگر به‌صورت اتوماتیک از نسخه امن آن سرویس استفاده خواهد کرد.

برای مطالعه بیشتر و توضیحات کامل درباره این افزونه (به زبان فارسی) می‌توانید به اینجا مراجعه کنید:

http://www.dw.de/dw/article/0,,15342696,00.html

مطلبی که در بالا لینک آن را می‌بینید، اطلاعات مهم و کاربردی دیگری هم درباره افزایش امنیت دیجیتال ارائه کرده است.

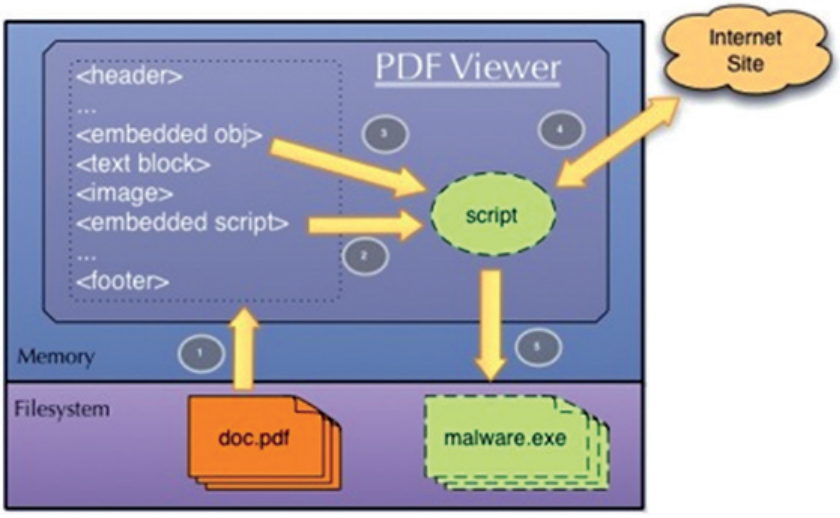


بدافزارها و نرم‌افزارهای شرکت Adobe

نرم‌افزارهای شرکت Adobe مانند Flash Player Acrobat، و غیره تقریبا روی همه کامپیوترهای شخصی نصب شده‌اند. همین ویژگی هکرها را به سمت سوء استفاده از نرم‌افزارهای کهنه و قدیمی شرکت Adobe برده است.

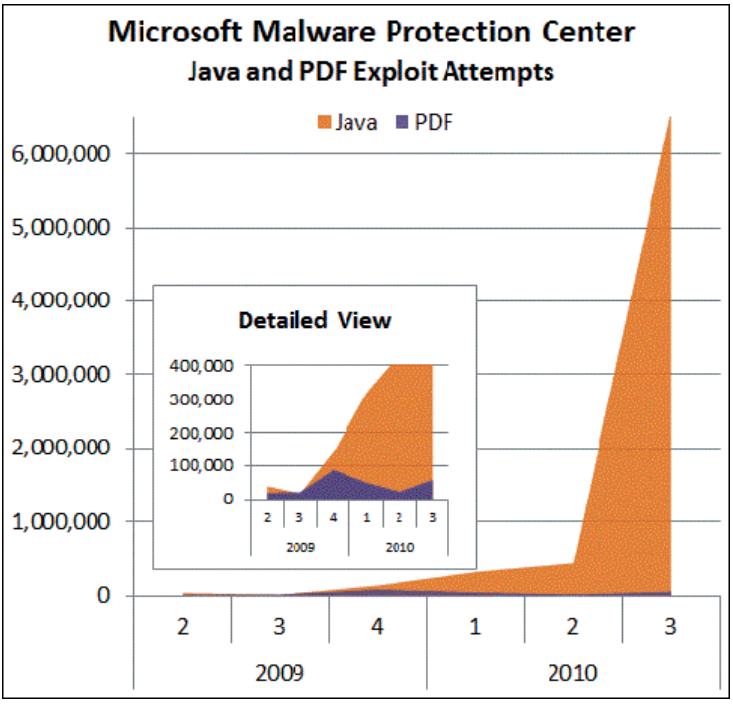
همانطور که در شکل روبرو مشاهده می‌کنید سهم بدافزارهایی که برای انتقال با نرم‌افزار آکروبات طراحی شده‌اند از ۲ درصد در سال ۲۰۰۸ به ۲۸ درصد در سال ۲۰۱۰ رسیده است. آکروبات خود را دائما به روزرسانی کنید.

فایل‌های پی‌دی‌اف را با دقت بیشتر بررسی کرده و اسکن کرده و از پذیرش فایلهای پی‌دی‌اف از افراد ناشناس خودداری کنید. درست مانند خطرات آکروبات، نرم‌افزار فلش از شرکت Adobe می‌تواند حاوی همان خطرات و بدافزارها باشد.



خطری به نام جاوا

اجرای چشم بسته و بدون کنترل اسکریپت‌های جاوا، ساده‌ترین راه برای آلوده شدن به انواع و اقسام بدافزارهاست. تصویر صفحه بعد، رشد انفجارگونهٔ حملات متکی به جاوا اسکریپت را در سال‌های گذشته نمایش داده و با خطرات ناشی از فایل‌های پی‌دی‌اف آلوده مقایسه می‌کند.



پیشنهاد برای مقابله با بدافزارهای جاوا:

- اگر کامپیوتر شما دارای اطلاعات فوق‌العاده حساس است، جاوا را اساسا uninstall کنید؛ جاوا برای اغلب صفحات اینترنتی مسئله مرگ و زندگی نیست.
- تنظیمات مرورگر خود برای حساسیت روی امنیت جاوا را به حداکثر افزایش دهید.
- از افزونه‌هایی مثل no-script برای فایرفاکس استفاده کنید و یا برای صفحات غیرناشناس از حالت incognito در کروم
- مایکروسافت در حال ساخت ابزاری به نام Zozzle است که بدافزارهای جاوا را تشخیص می‌دهد.

حملات اینترنتی Cross-site scripting (XSS)

در سال‌های گذشته، گروه موسوم به ارتش سایبری سپاه پاسداران، از روش Cross-site scripting برای بسیاری از حملات خود نظیر هک سایت‌های بالاترین، سازگارا و رادیو زمانه استفاده نموده است.

حملات Cross-site scripting غالبا به شیوه زیر انجام می‌پذیرند:

فرض کنید نام کاربری و رمز عبور پست الکترونیکی جی‌میل خود را وارد کرده مشغول بررسی ایمیل‌های خود هستید، در این حالت جی‌میل با ارسال و نصب تعدادی کوکی، برخی از اطلاعات ورودی شما را جمع‌آوری می‌کند. حمله‌کنندگان با ارسال ایمیلی حاوی یک کد آلوده به شما، پس از دریافت و فعال شدن این ایمیل با سوء استفاده از آسیب‌پذیری صفحاتی نظیر جی‌میل، برخی از اطلاعات

محرمانه کوکی‌های جی‌میل را از کامپیوتر شما سرقت نموده و سپس با استفاده از این اطلاعات وارد حساب ایمیل می‌شوند. در عملیات ارتش سایبری از ایمیل‌های هک شده برای مراجعه به شرکت‌های ثبت دامنه سایت‌ها استفاده شده بود، حمله‌کنندگان با ادعای فراموش کردن رمز عبور، از شرکت‌های ثبت دامنه خواسته بودند تا رمز عبور جدیدی برایشان ارسال کند.

اگر چه به گفته متخصصان امنیت در گوگل، آسیب‌پذیری جی‌میل برطرف شده است، اما امکان حملات Cross-site scripting هیچگاه منتفی نیست. قربانیان حملات Cross-site scripting می‌توانستند با غیرفعال کردن امکان نمایش تصاویر و فایل‌های الصاقی در حساب ایمیل خود، احتمالا جلوی اجرای بدافزار ارسالی حمله‌کنندگان را سد کنند. راه حل دیگر نگهداری اطلاعات فوق حساس نظیر اطلاعات مربوط به دامین‌ها و هاست‌ها بر روی ایمیلی مخفی است که معمولا از آن استفاده روزمره نمی‌کنید و البته امنیت بسیار بالایی دارد.

پیشنهادهایی برای مقابله با حملات XSS

۱. کروم و یا فایرفاکس را برای سایت‌های ناشناس در حالت incognito یا private تنظیم نمائید.

۲. برای کامپیوترهای حساس یا از Java استفاده نکنید یا افزونه‌هایی مانند NotScripts را روی کروم و یا فایرفاکس نصب کنید.

۳. فلش هم نوعی جاوااسکریپت است، استفاده از فلش‌های ناشناس ریسک آلوده شدن دارد.

۴. به آدرس لینک‌ها دقت کنید، سایت‌های آلوده را با لینک‌های آشنا برای شما می‌فرستند؛ مثلا به جای https://www.google.com/ ممکن است لینکی به صورت https://www.googles.com/ برای شما ارسال شده باشد که با کمی‌دقت متوجه تفاوت خواهید شد.

۵. مهاجمان پیشرفته می‌توانند بدافزارهای خود را حتی داخل تصاویر نیز مخفی کنند. راهی برای تضمین صد درصدی امنیت وجود ندارد. فایل‌های Cache مرورگر خود را دائما پاک کنید. رفتار فایل‌های باز در حافظه را کنترل نمائید.

Comodo Secure DNS

سوال: چرا به دانشجویان خود استفاده از Comodo Secure DNS را توصیه کنم؟

استفاده از Comodo Secure DNS اولا سریع است، سرورهای کمودو در پنج قاره جهان به صورت راهبردی به شکلی پراکنده شده‌اند که در کوتاه‌ترین مدت زمان ممکن، دامنه مورد نظر شما را پیدا می‌کنند.

ثانیا Comodo Secure DNS برخی از عمده‌ترین خطرات متوجه کامپیوتر شما را شناسایی و رفع می‌کنند. در صورت استفاده از Comodo Secure DNS، شرکت کمودو به عنوان یکی از شرکت‌های بزرگ و پیشروی خدمات امنیت سایبری، توسط Comodo Secure DNS به شما قبل از ورود به سایت‌های زیر هشدار می‌دهد:

- سایت‌های منتشرکننده فیشینگ

- سایت‌های منتشرکننده بدافزارها
- سایت‌های بمباران‌کننده با تبلیغات
- سایت‌های منتشرکننده جاسوس‌افزارها

همه دلایل فنی توصیه استفاده از Comodo Secure DNS خصوصا به دانشجویان ساکن ایران در حوصله این بحث نمی‌گنجد. سازمان‌ها و ارگان‌های خاصی در ایران و متأسفانه ISPهای عموما مرتبط با همان سازمان‌ها و ارگان‌ها، سابقه دستکاری DNS و در مواردی Large scale DNS Cache Poisoning را دارند. استفاده از Comodo Secure DNS تا حدی خطر این تهدید مشخص را کاهش می‌دهد.

برای نصب Comodo Secure DNS کافیست دو آدرس DNS خود را از حالت اتوماتیک خارج کرده و به آدرس‌های زیر تبدیل کنید:

Preferred DNS server address for Comodo Secure DNS is: 8.26.56.26
Alternate DNS server address for Comodo Secure DNS is: 8.20.247.20

این کار را می‌توانید در تنظیم پروتکل TCP/IP واسط کامپیوتر خود با اینترنت، مثلا کارت شبکه یا مودم وایرلس و از آن بهتر، روی Router خود انجام دهید تا مستقیما برای کامپیوترهای متصل به Router اعمال شود.

اگر نحوه تغییر آدرس DNSها را نمی‌دانید روی لینک‌های زیر کلیک کنید:

Windows Vista Instructions
Windows XP Instructions
Mac OS X Instructions
Router Instructions

به روز رسانی سیستم عامل

به روز رسانی سیستم عامل مهمترین و تاکید می‌کنم مهمترین رکن امنیت کامپیوتر شماست، ارائه کنندگان سیستم عامل مثلا مایکروسافت بعضا روزانه patchها و بسته‌های تکمیلی برای بستن حفره‌های امنیتی نرم‌افزار خود ارائه می‌نمایند.

از دانشجویان با تأکید بخواهید به سیستم عامل اجازه دهند به صورت اتوماتیک به روز رسانی شود.

کنترل به روز رسانی نرم‌افزارها با Secunia

بدون اطمینان از به روز بودن همه نرم‌افزارهای سیستم شما، صحبت از امنیت کامپیوتری بی‌معناست. نرم‌افزارهایی چون فلش پلیر، آکروبات ریدر، نرم‌افزار Winzip یا Rar و Real Player بر روی بیشتر کامپیوترهای شخصی یافت می‌شوند. تبهکاران با دستکاری نسخه‌های قدیمی این نرم‌افزارها، راه نفوذ به کامپیوتر قربانیان را باز می‌کنند. شرکت‌های سازنده نرم‌افزار با به روز رسانی مرتب برنامه‌های خود به سرعت آسیب‌پذیری‌ها و ایرادات امنیتی محصولات خود را بهبود می‌بخشند، به همین خاطر توصیه می‌شود تمامی برنامه‌های نرم افزاری (Software) و یا میان‌افزاری (Firmware) کامپیوتر خود را دائما به روز رسانی کنید. این برنامه‌ها می‌تواند از Windows Update تا یک داریور ساده برای مودم کامپیوتر شما باشد.

سایت Secunia امکان اسکن و جستجوی آنلاین آسیب‌پذیری‌های کامپیوتر شما را فراهم آورده است با ورود به این سایت در آدرس http://secunia.com/vulnerability_scanning می‌توانید کامپیوتر خود را در جستجوی نرم‌افزارهای حامل ریسک و خارج از رده بکاوید.

مهمترین نرم‌افزارها برای به روز رسانی عبارتند از:

- سیستم عامل
- ضدویروس و نرم‌افزارهای ضدجاسوس
- مرورگرها
- نرم‌افزارهای واژه‌پرداز نظیر وُرد
- نرم‌افزارهای عمومی پرطرفدار نظیر آکروبات

Secunia دو نرم افزار رایگان به نام‌های OSI و PSI را برای ارتقاء امنیت کامپیوتر شما عرضه کرده است. برنامه رایگان اول (OSI) کامپیوتر شما را بدون نصب نرم‌افزاری خاص و از طریق وصل شدن به سایت Secunia اسکن می‌کند. برنامه دوم (PSI) بسته نرم‌افزاری رایگانی است که پس از نصب، کامپیوتر شما را به دنبال برنامه‌های خارج از رده و پلاگین‌های قدیمی و آسیب‌پذیر جستجو می‌کند.


Welcome to Secunia Online Software Inspector (OSI)
Scan Now
The Secunia Online Software Inspector will inspect your operating system and software for insecure versions and missing security updates. A default inspection normally lasts 5-40 seconds, while a thorough inspection may take several minutes.
Detection Statistics:
15 Applications Detected in Total
4 Insecure Versions Detected
11 Patched Versions Detected
Start
Stop
Scan Options:
Enable thorough system inspection
Display only insecure programs
Running For:
7 Minutes, 45 Seconds
Errors with the scan:
0 Errors Detected, scan result should be correct
Status / Currently Processing:
C:\Windows\SoftwareDistri...005_none_670656a59d28c52a
Programs / Result
Version Detected
Status
Adobe Reader 9.x
9.0.0.332
This installation of Adobe Reader 9.x is insecure and potentially exposes your system to security threats!
The detected version installed on your system is 9.0.0.332, however, the latest patched version released by the vendor, fixing one or more vulnerabilities, is 9.3.0.0.
Installed on Your System in:
C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
Adobe Flash Player 9.x
9.0.124.0 (ActiveX)
This installation of Adobe Flash Player 9.x is insecure and potentially exposes your system to security threats!
The detected version installed on your system is 9.0.124.0 (ActiveX), however, the latest patched version released by the vendor, fixing one or more vulnerabilities, is 9.0.277.0 (ActiveX).
Update Instructions:
Download
Installed on Your System in:
C:\Windows\SYSTEM32\Macromed\Flash\Flash9f.ocx
Google Chrome 5.x
5.0.375.86
This installation of Google Chrome 5.x is insecure and potentially exposes your system to security threats!
The detected version installed on your system is 5.0.375.86, however, the latest patched version released by the vendor, fixing one or more vulnerabilities, is 5.0.375.99.
Update Instructions:
Download
Installed on Your System in:
C:\Users\nima\AppData\Local\Temp\..\application data\google\Chrome\Application\5.0.375.86\chrome.dll
Sun Java JRE 1.6.x / 6.x
6.0.170.4
This installation of Sun Java JRE 1.6.x / 6.x is insecure and potentially exposes your system to security threats!
The detected version installed on your system is 6.0.170.4, however, the latest patched version released by the vendor, fixing one or more vulnerabilities, is 6.0.200.2.
Update Instructions:
Download

Cloud Computing

در تکنولوژی پردازش ابری، روز به روز وابستگی شما به دستگاه‌های ذخیره‌سازی اطلاعات نظیر هارد دیسک کاهش یافته، اطلاعات و حتی برنامه‌های کاربردی شما روی سرورهای ابر، ذخیره و یا اجراء می‌شوند.

شما احتمالا با پردازش و ذخیره‌سازی ابری، آشنایی دارید. سال‌ها پیش از ظهور جی‌میل، سرویس ایمیل گوگل، برنامه‌هایی نظیر Outlook ایمیل‌های شما را از سرور ایمیل شما دانلود و روی هارد دیسک ذخیره می‌کردند، امروز جی‌میل، پست الکترونیکی شما را ذخیره می‌کند و نیاز چندانی به ذخیره‌سازی ایمیل‌ها روی هارد دیسک نیست. سرویس‌های آنلاین دیگر گوگل نظیر Google Docs نیز تلاش دارند جایگزین برنامه‌های آفلاین مشابه نظیر Microsoft Office شوند به همین دلیل شرکت مایکروسافت نیز با ورود به این عرصه برنامه‌هایی نظیر Office 365 را ارائه نموده است.

مشاهده این ویدئو می‌تواند به افزایش امنیت Google Docs شما کمک شایانی کند:

http://www.youtube.com/watch?v=qo-ZrbrAhDI

استفاده از «ابر» را به دو شرط ذیل توصیه می‌کنیم:

الف. به اینترنت پرسرعت دسترسی دارید.

ب. شیوه مناسبی برای حفظ رمزهای کامپیوتر خود نزد دوستان و بستگان خود در خارج از ایران یافته‌اید.

شما در صورت دسترسی به اینترنت پرسرعت می‌توانید، داده‌های حساس، ایمیل‌ها، تصاویر، موزیک و ویدئوی خود را روی «ابر» ذخیره نموده با دوستان خود به اشتراک گذارید. یکی از مشهورترین این سرویس‌ها Dropbox است. ترکیبی از Dropbox و TrueCrypt می‌تواند برای شما فضای ذخیره‌سازی آنلاین به علاوه امکانات کدگذاری را فراهم آورد. توجه داشته باشید که سرویس‌های مشابهی امکان ذخیره اطلاعات کدگذاری شده را ارائه می‌دهند، فهرست سرویس‌های Backup و ذخیره‌سازی آنلاین را از این آدرس می‌توانید مشاهده نمایید.

http://en.wikipedia.org/wiki/List_of_online_backup_services

امنیت حافظه‌های فلش، USB Drive یا کول دیسک

اطلاعات خود را به صورت کدگذاری شده روی درایوهای فلش ذخیره کنید تا در صورت سرقت یا گم شدن حافظه فلش اطلاعات شما به راحتی قابل دستیابی نباشند. دو نرم‌افزار پیشنهادی برای کدگذاری عبارتند از BitLocker to Go و TrueCrypt.

در بازار حافظه‌های فلش نظیر Ironkey وجود دارند که خود اطلاعات را کدگذاری می‌کنند. در برخی موارد اگر کسی پسورد را چند بار اشتباه وارد کند. حافظه فلش اطلاعات شما را به صورت خودکار از میان می‌برد.

حالت Autorun هارد دیسک‌های اکسترنال و حافظه‌های فلش را خاموش کنید. بسیاری از این دیسک‌ها، خصوصا دیسک‌های ناشناس حاوی خطرات جدی مثل تروجان‌ها هستند و به محض اتصال به کامپیوتر شما، بدافزارها را به صورت خودکار نصب می‌کنند.

کدگذاری داده‌ها با TrueCrypt

نرم‌افزار رایگان کدگذاری TrueCrypt به صورت رایگان شما را قادر به کدگذاری حافظه‌های فلش، هارد دیسک و هر نوع حافظه ذخیره‌سازی می‌کند. استفاده از TrueCrypt داده‌های شما را در برابر تلاش برای ورود با تایپ مجدد پسورد یا نرم‌افزارهای پسوردشکن ایمن می‌کند.

TrueCrypt از مهم‌ترین برنامه‌های رمزگذاری و پنهان‌سازی فایل‌ها است و امکانات بسیار جالب و کم‌نظیری به کاربران ارائه می‌دهد. از اینجا می‌توانید به زبان فارسی جزئیات نصب آن را بخوانید:

http://www.tafreevar.com/2603/truecrypt-safe-place-critical-information

مطالعه بیشتر

فهرست ذیل حاوی عمومی‌ترین متدهای ارتش سایبری جمهوری اسلامی ایران و دیگر تبهکاران اینترنتی روی سایت‌های آلوده است.

SQL injection
Cross-Site Scripting (XSS)
HTTP Response Splitting
Open Redirect
Command Injection
Code Injection
Directory Traversal
XPATH Injection
LDAP injection
Forced Browsing
Blind SQL Injection

برای مطالعه بیشتر دربارهٔ مشخصات و نحوه مقابله با این حملات می‌توانید از منابع زیر استفاده کنید:

http://www.imperva.com/docs/HII_An_Anatomy_of_a_SQL_Injection_Attack_SQLi.pdf

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

http://vimeo.com/28268598

http://www.slideshare.net/eoftedal/avoiding-cross-site-scripting-not-as-easy-as-you-might-think

http://www.slideshare.net/fmavituna/how-to-detect-xss

http://resources.infosecinstitute.com/http-response-splitting-attack/

http://www.slideshare.net/innotech_conference/owasptop-10

http://www.acunetix.com/websitesecurity/cross-site-scripting.htm

http://www.cgisecurity.com/xss-faq.html

http://www.net-security.org/dl/articles/Javascript_malware.pdf

http://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf

http://www.acunetix.com/websitesecurity/directory-traversal.htm

۵

مقابله با بدافزارها

در بخش‌های پیشین گفتیم که بدافزارها سال‌هاست تنها محدود به ویروس‌ها نمی‌شوند، در واقع مثلا تهدیدهای بسیار جدی‌تر مانند تروجان‌ها تا سه برابر ویروس‌ها کامپیوترهای شخصی را آلوده می‌کنند و به دلایلی که توضیح داده شد در بیشتر موارد از ویروس‌ها خطرناک‌ترند.

در سال‌های گذشته ضدویروس‌های بسیار موثر و در عین حال رایگانی ارائه شده است. خدمات آنتی‌ویروس‌ها به دو شکل آنلاین و آفلاین قابل دسترسی است.

آنتی‌ویروس‌های آنلاین

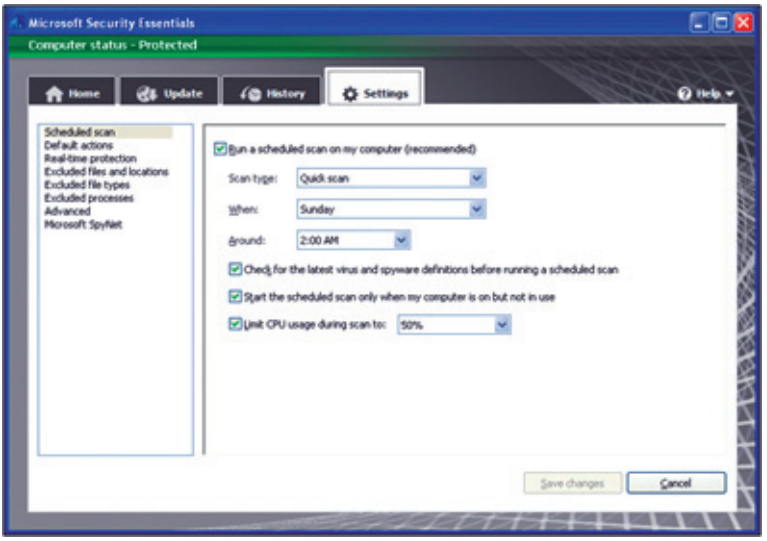
اگر با سیستمی مواجهید که احتمال می‌دهد آلوده شده باشد و اگر این سیستم آنتی‌ویروس ندارد و یا احتمال می‌دهید، بدافزاری نرم‌افزار آنتی‌ویروس قدیمی و یا معیوب سیستم را غیرفعال کرده باشد. بهتر است در ابتدا از یک آنتی‌ویروس آنلاین استفاده کنید. ناگفته پیداست که آنتی‌ویروس‌های آنلاین نیازمند یک ارتباط پرسرعت اینترنت هستند. آنتی‌ویروس‌های آنلاین زیر برای شروع پیشنهاد می‌شوند:

۱. آنتی‌ویروس Panda Active Scan از شرکت Panda Security

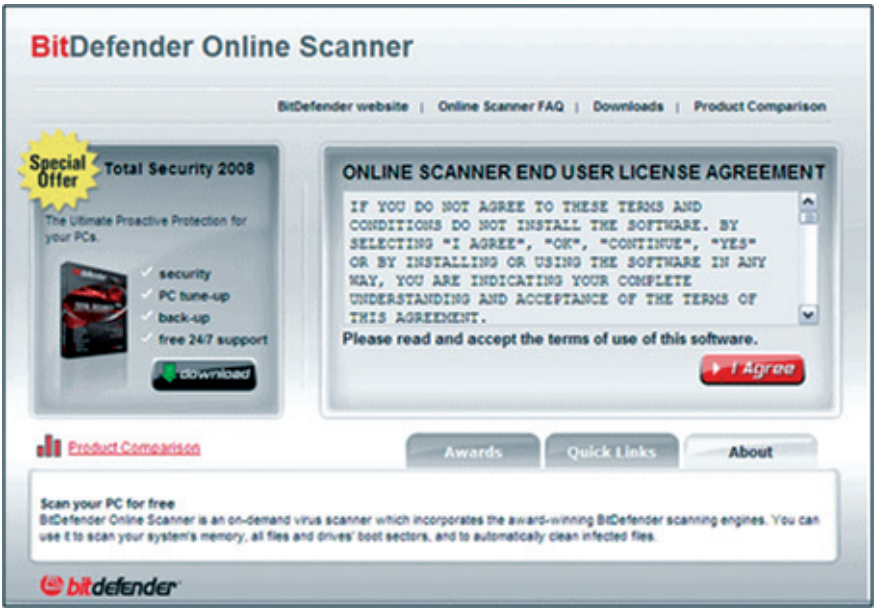
آدرس:

http://www.pandasecurity.com/homeusers/solutions/activescan/

۲. آنتی‌ویروس Microsoft Safety Scanner از شرکت Microsoft
آدرس: http://www.microsoft.com/security/scanner/en-us/default.aspx

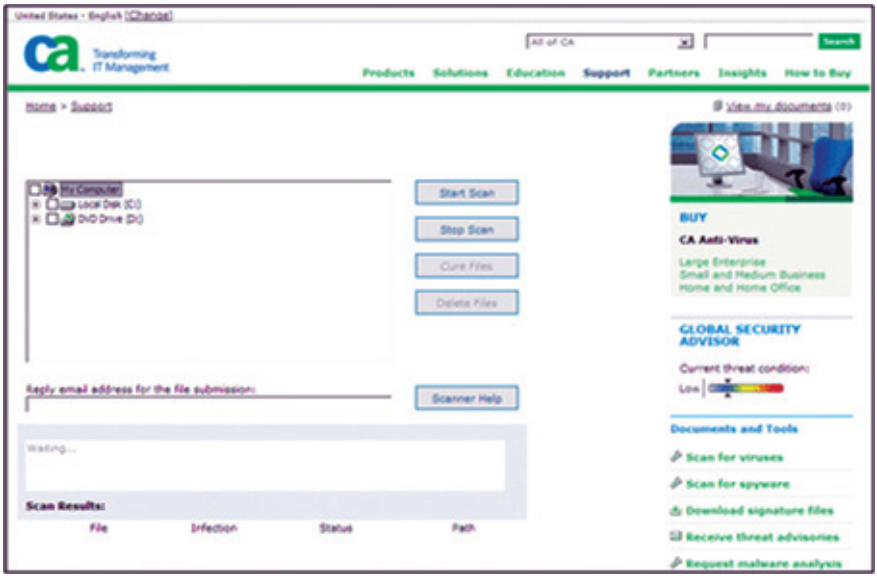


۳. آنتی‌ویروس Online Bitdefender از شرکت Bitdefender
آدرس: http://www.bitdefender.com/scanner/online/free.html
این شرکت برای اکثر مرورگرها، افزونه امنیت وب نیز ارائه کرده است.



۴. آنتی‌ویروس Computer Associates Malware Scanner که تنها روی اینترنت اکسپلورر اجرا می‌شود.

آدرس: http://cainternetsecurity.net/entscanner/

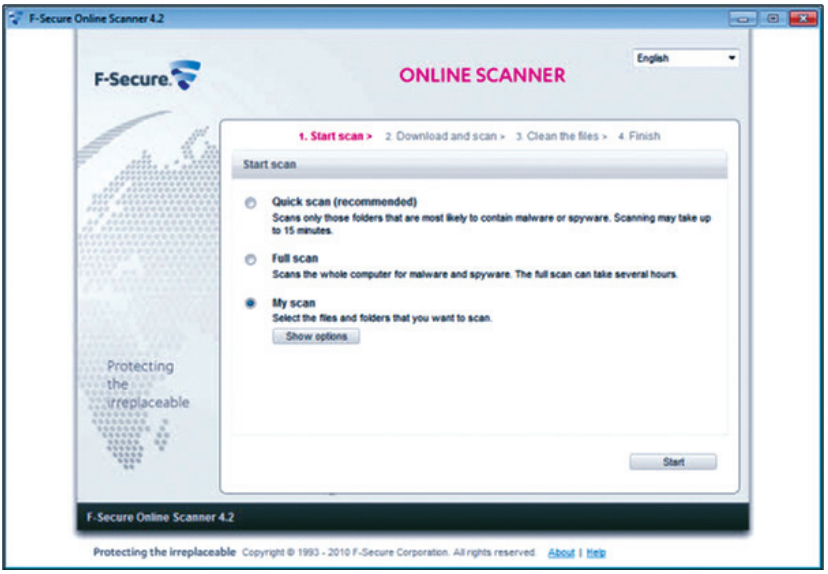


۵. آنتی‌ویروس آنلاین ESET از شرکت Eset.com

آدرس: http://www.eset.com/us/online-scanner/

۶. آنتی‌ویروس آنلاین housecall از شرکت TrendMicro
آدرس: http://housecall.trendmicro.com/

۷. آنتی‌ویروس آنلاین online scanner از شرکت F-Secure که آنتی‌ویروس کوچکی است و با Active X و جاوا کار می‌کند.
آدرس: http://www.f-secure.com/en/web/labs_global/removal/



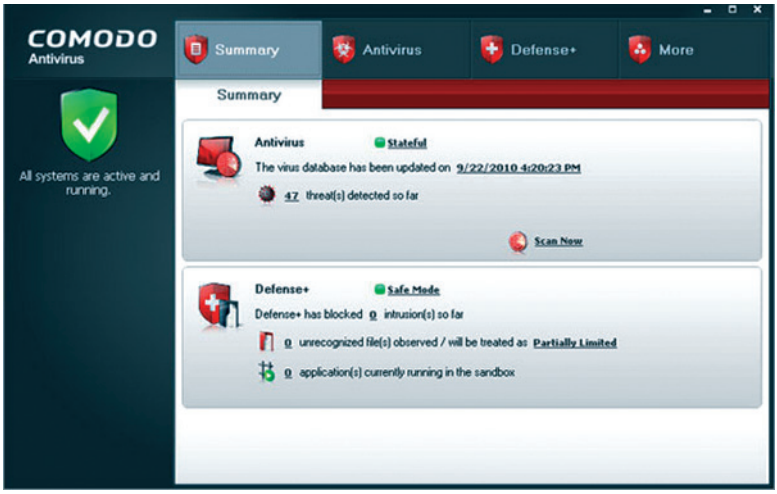
آنتی‌ویروس‌های فوق الذکر پاسخگوی نیاز ۹۹ درصد کاربران عادی است. به دانشجویان توصیه کنید از جستجو به دنبال آنتی‌ویروس آنلاین در موتورهای جستجو خودداری کنند. موتورهای جستجو صدها آنتی‌ویروس به شما معرفی می کنند که بسیاری از آنان آنتی‌ویروس‌های تقلبی یا Rogue security software هستند. Rogue security softwareها از جمله عمده‌ترین تهدیدها علیه امنیت کاربران کامپیوترهای شخصی‌اند که تعدادشان در سال‌های اخیر رشدی انفجاری داشته است. به دانشجویان توصیه کنید قبل از نصب و یا استفاده از هر نوع آنتی‌ویروس از طریق سایت‌های معتبر نظیر سیمانتک یا مک‌آفی یا حداقل ویکی‌پدیا از امنیت آن اطمینان حاصل کنند. ویکی‌پدیا فهرستی از آنتی‌ویروس‌های تقلبی را در آدرس زیر ارائه کرده است:
http://en.wikipedia.org/wiki/Rogue_security_software

آنتی‌ویروس یا نرم‌افزارهای مقابله با بدافزار

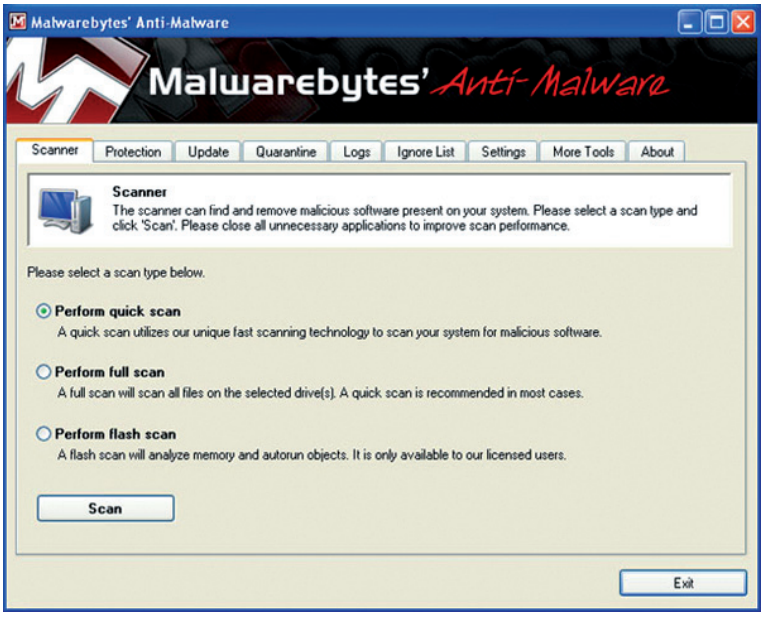
ما در اینجا گروهی از آنتی‌ویروس‌های برگزیده و رایگان را برای استفاده توسط کاربران عادی معرفی می‌کنیم. نکته حائز اهمیت اینکه کاربران تجاری و سازمان‌ها بهتر است از آنتی‌ویروس‌های حرفه‌ای غیررایگان با امکان خدمات تلفنی استفاده نمایند.

آنتی‌ویروس‌های موثر و رایگان

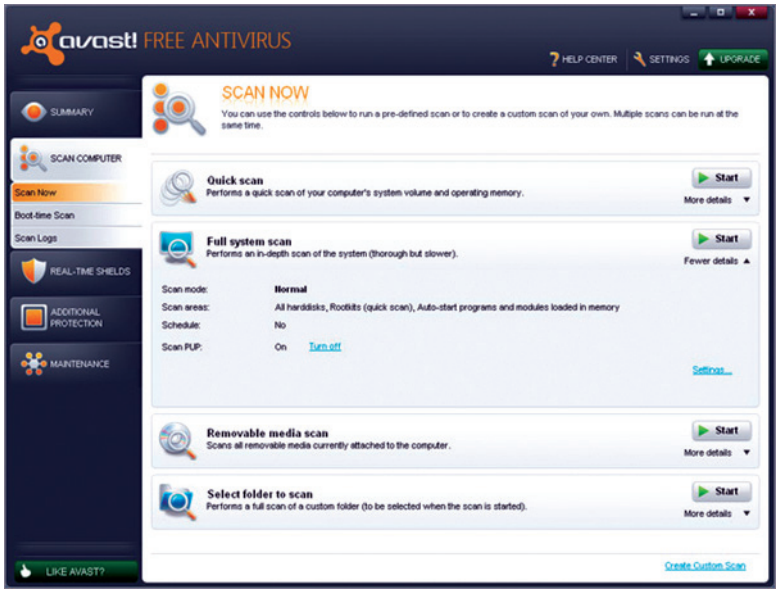
۱. بسته نرم‌افزاری امنیت اینترنتی از شرکت کمودو، comodo free internet security که مشخصات آن در همین بخش توضیح داده خواهد شد.
آدرس برای دانلود:
http://www.comodo.com/home/internet-security/free-internet-security.php



۲. بسته نرم‌افزاری Malwarebytes، حاوی آنتی‌ویروس قدرتمند و برنامه ضدجاسوس
آدرس برای دانلود: http://www.malwarebytes.org/



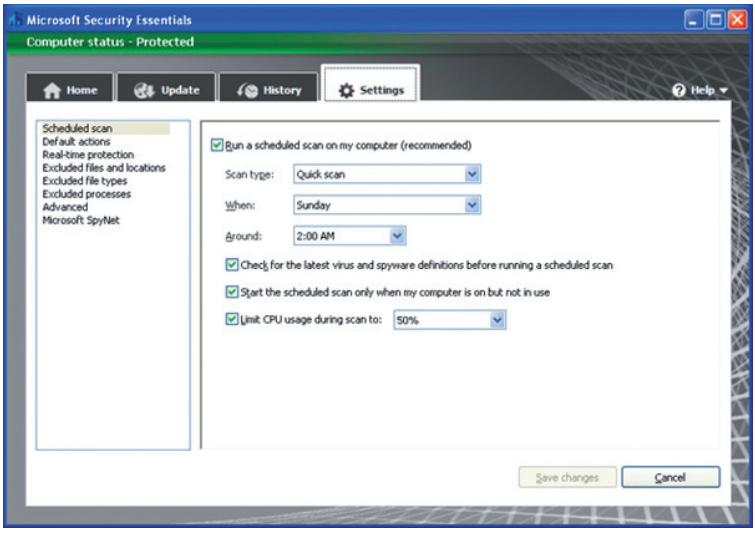
۳. بسته نرم‌افزاری Avast! Free Antivirus، از بسته امنیتی توصیه شده توسط گوگل
آدرس برای دانلود: http://www.avast.com/free-antivirus-download



۴. بسته نرم‌افزاری Microsoft Security Essentials، پروژه ضدویروس و مبارزه با بدافزارها از شرکت مایکروسافت

آدرس برای دانلود:

http://windows.microsoft.com/en-GB/windows/products/security-essentials



۵. بسته نرم‌افزاری AVG Free، آنتی‌ویروس منتخب بسیاری از سایت‌های ارزیابی آنتی‌ویروس‌ها که نرم‌افزاری سریع و کوچک است.

آدرس برای دانلود: http://free.avg.com

۶. بسته نرم‌افزاری Avira، آنتی‌ویروس رایگان، ساده و قدرتمند
آدرس برای دانلود: http://www.avira.com/en/avira-free-antivirus

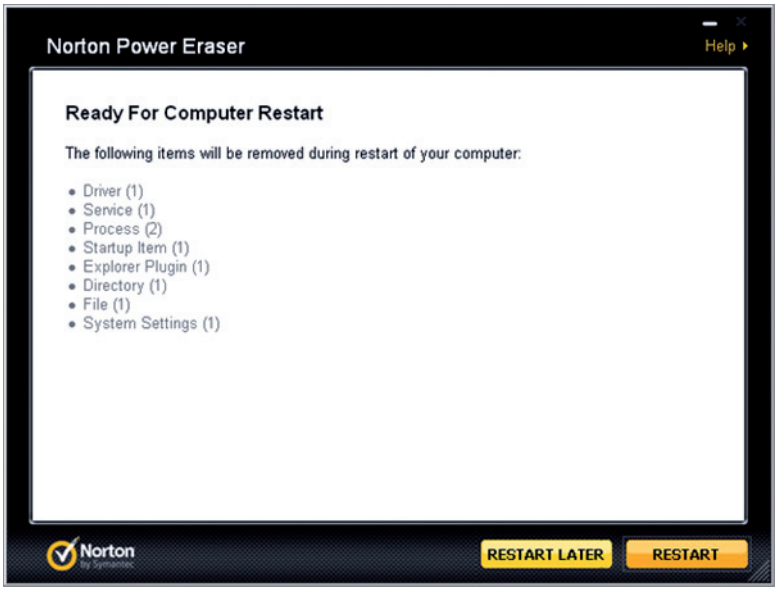
۷. بسته نرم‌افزاری Adware Free از شرکت Lavasoft، آنتی‌ویروس قدرتمند با قدرت مقابله همزمان برنامه‌های جاسوس و روت‌کیت‌ها
آدرس برای دانلود: http://www.lavasoft.com/products/ad_aware_free.php

۸. بسته نرم‌افزاری Panda Cloud Antivirus Free Edition از شرکت panda security، یکی از پرطرفدارترین بسته‌های رایگان مقابله با بدافزارها

آدرس برای دانلود: http://www.cloudantivirus.com/en/

۹. برنامه Norton Power Eraser از شرکت Symantec

آدرس برای دانلود: http://security.symantec.com/nbrt/npe.aspx?



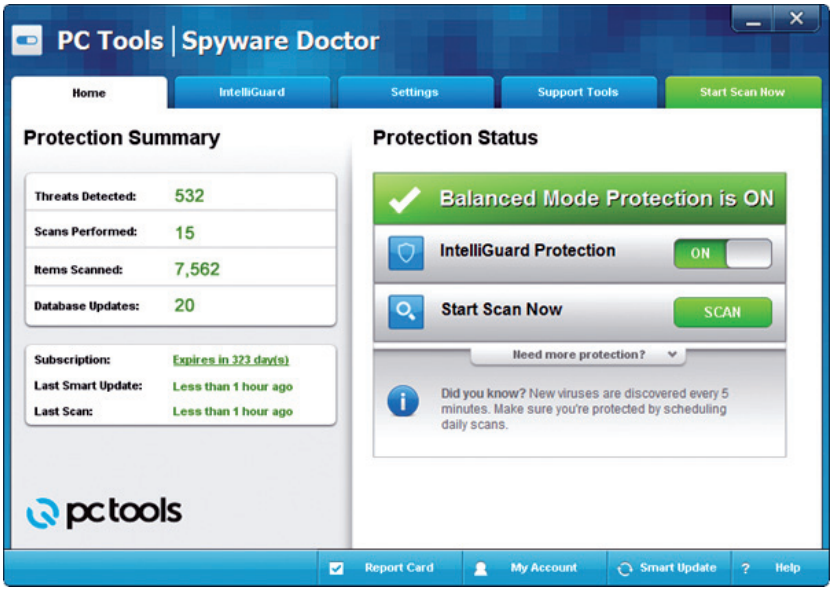
برای استفاده از این برنامه توجه به نکات زیر ضروری است:

این برنامه از روش بسیار «افراطی» و تهاجمی یا aggressive برای مقابله با بدافزارها استفاده می‌کند، استفاده از این برنامه برای کاربران عادی توصیه نمی‌شود چرا که ممکن است فایل‌های غیرمضر را بدافزار تشخیص دهد. پیشنهاد می‌شود فایل‌های مضر اعلام شده توسط برنامه را یک به یک مطالعه و در صورت اطمینان کامل از بدافزار بودن پاک کنید.

این برنامه در عین حال بسیار موثر است و در اغلب موارد بدافزارهایی را تشخیص می‌دهد که آنتی‌ویروس‌های دیگر آنان را شناسایی نمی‌کنند. یکی از کاربردهای دیگر این برنامه زمانی است که بدافزار به آنتی‌ویروس‌های دیگر اجازه نصب شدن نمی‌دهد و به اصطلاح آن‌ها را بلوکه می‌کند. در این حالت این برنامه می‌تواند با restart کردن کامپیوتر شما به شکلی کارآمد سراغ بدافزارها رفته و آنها را پیدا کند.

۱۰. یکی از برنامه‌های پرکاربرد برای پاک‌کردن ابزارهای جاسوسی و تروجان‌ها، نرم‌افزار Spyware Doctor است. این نرم‌افزار را می‌توانید از اینجا دانلود کنید:

http://www.pctools.com/forum/showthread.php?69406-2012-Release-PC-Tools-Spyware-Doctor-and-PC-Tools-Spyware-Doctor-with-AntiVirus-v9



نکات مهم در استفاده از نرم‌افزارهای آنتی‌ویروس

• نصب نرم‌افزار آنتی‌ویروس کمک زیادی به کامپیوتری که به اینترنت وصل نیست نمی‌کند، هر روز ده‌ها بدافزار جدید تولید و پراکنده می‌شوند. شرکت‌های تولیدکننده آنتی‌ویروس نیازمند آپدیت کردن مداوم و به روز رسانی نرم‌افزارهای خود هستند. لذا امکان به روز رسانی اتوماتیک آنتی‌ویروس خود را همیشه فعال نگاه دارید.

• نرم‌افزار ضدویروس، فایروال و تکنولوژی +Defense بسته نرم‌افزاری Comodo Internet Security که به رایگان ارائه می‌شوند در میان نرم‌افزارهای موجود قدرت و کنترل بسیار بالایی را در اختیار کاربر با اطلاعات پیشرفته از امنیت سایبری قرار می‌دهند. بهتر است به جای استفاده از فایروال و آنتی‌ویروس‌های مختلف، از کمودو استفاده کنید.

• نسبت به پیام‌های آنتی‌ویروس خود حساس باشید، مطمئن شوید که معنای نحوه مواجهه با فایل‌های آلوده را می‌فهمید. پاک کردن بسیاری از فایل‌های آلوده نیازمند Restart کردن سیستم است، بسته آنتی‌ویروس شما در این صورت از شما خواهد خواست سیستم خود را راه‌اندازی مجدد کنید.

• بر روی یک کامپیوتر شخصی دو آنتی‌ویروس نصب نکنید. این کار موجب اخلال در منابع سیستم می‌شود.

• در عین حال می‌توانید حتی روی کامپیوتری که نرم‌افزار آنتی‌ویروس نصب کرده‌اید هر چند روز یک‌بار یکی از آنتی‌ویروس‌های آنلاینی را که معرفی شد اجراء و تست نمائید. شاید جالب به نظر آید که در بعضی مواقع اجرای چند آنتی‌ویروس آنلاین خصوصا درباره روت‌کیت‌ها موفقیت‌آمیزتر از اعتماد به یک برنامه ضدویروس خواهد بود.

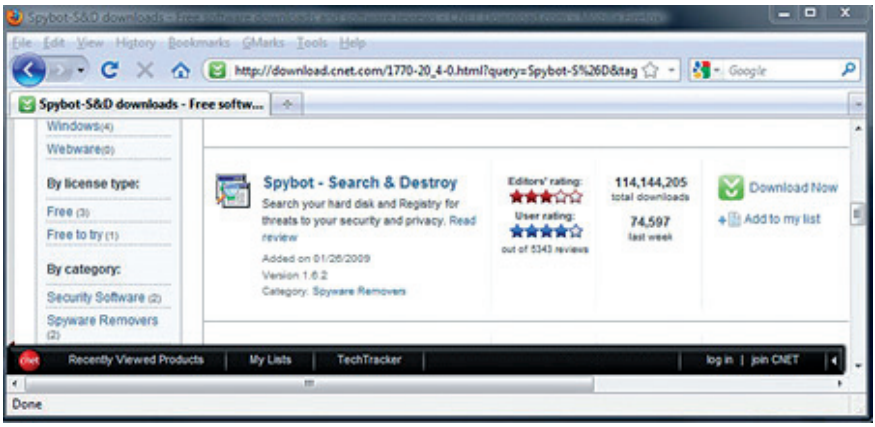
• از فایل‌های مورد نیاز خود دائما نسخه پشتیبان تهیه کنید. اگر ویروس‌ها فایل‌های شما را تخریب کنند شاید پاک کردن کامل فایل از ویروس امکان‌پذیر نباشد و فایل‌ها بایستی اساسا پاک شوند.

• اگر برای پاک کردن یک کامپیوتر ویروسی می‌روید که امکان دسترسی به اینترنت را ندارد، یک سی‌دی یا فلش‌دیسک write protect تهیه کنید. آخرین نسخه آنتی‌ویروس مثلا پاندا را روی سی‌دی کپی کنید، دقت کنید که CD به اصطلاح بسته شده باشد و قابلیت افزوده شدن اطلاعات یا rewrite نداشته باشد. برای پاک‌سازی کامپیوتر قربانی حملات بدافزار، آنتی‌ویروس را از روی سی‌دی install کنید.

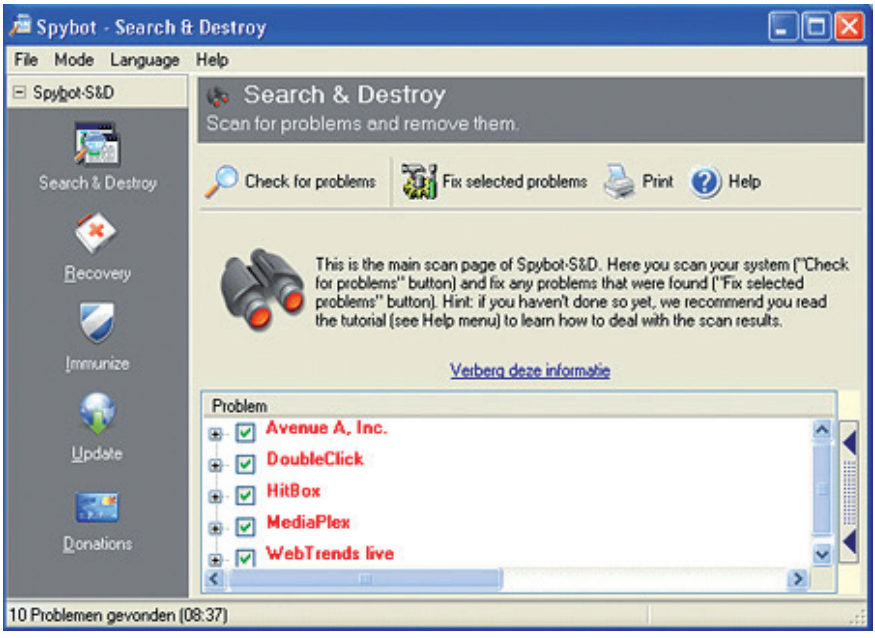
مقابله با جاسوس‌افزارها با Spybot - Search & Destroy

نرم‌افزار Spybot - Search & Destroy از محبوب‌ترین برنامه‌های مقابله با جاسوس‌افزارها است. از سایت عرضه‌کننده این برنامه به آدرس http://www.safer-networking.org/en/download می‌توان این برنامه را دانلود کرد. این برنامه را همچنین از سایت‌های بزرگ دانلود نرم‌افزارهای ایمن مانند

http://download.cnet.com دانلود کرد.



پس از نصب و به روز رساندن این برنامه، بهتر است یک بار سراسر هارد دیسک کامپیوتر خود را برای یافتن جاسوس‌افزارهای احتمالی جستجو (اسکن) کنید. در صورت وجود چنین بدافزارهایی نتایج جستجو این‌گونه به نظر می‌رسد:



با انتخاب گزینه Fix selected problems می‌توانید بدافزارها را از حافظه کامپیوتر خود پاک کنید. امکان دیگر این برنامه حالت resident یا مانا، حالتی است که برنامه در حافظه کامپیوتر شما باقی می‌ماند

و به صورت دائم همه رفتارهای نرم‌افزارهای گوناگون را زیر نظر می‌گیرد. در صورتی که نرم‌افزاری رفتاری مشابه بدافزارها از خود نشان دهد، برنامه مقیم در حافظه از شما خواهد پرسید که آیا به سلامت برنامه مذکور اطمینان دارید یا خیر؟

امنیت اینترنتی با Comodo Internet Security

گرچه شهرت Comodo بیشتر به خاطر فایروال رایگان و توانمند آن است، اما بسته نرم‌افزار Comodo در واقع راه‌حلی کامل شامل آنتی‌ویروس و فایروالی پرقدرت و چندلایه است. فایروال کمودو بسیاری از نیازهای کاربران حرفه‌ای‌تر را برآورده می‌کند. به صورت لحظه‌ای لیستی از تمام ارتباطات کامپیوتر شما را ارائه می‌کند و شما قادرید این ارتباطات را محدود و یا متوقف کنید.

سه ابزار اصلی بسته نرم‌افزار امنیت اینترنتی کمودو عبارتند از AntiVirus، Firewall و +Defence.

این سه ابزار خصوصا فایروال و +Defence قابلیت بسیار وسیعی برای تنظیمات فوق‌العاده سخت‌گیرانه و در محیط‌های پرخطر یا تنظیمات پارانوئید (Paranoid) را دارند. این تنظیمات گرچه امنیت سیستم شما را به شکل قابل ملاحظه‌ای بهبود خواهند بخشید، اما شما را با سیلی از پرسش‌های مکرر در خصوص میزان اطمینان شما به امن بودن برنامه‌های متفاوت روبرو خواهد ساخت. تنظیمات فایروال و +Defence همان‌گونه که گفته شد بسیار گسترده و متفاوت‌اند. یادگیری تنظیمات این بسته نرم‌افزاری علاوه بر ارتقای امنیت کامپیوتر شما، شما را در فهم ارتباطات کامپیوتر نظیر پورت‌ها و نحوه دسترسی برنامه‌های مختلف به اینترنت یاری خواهد رساند.

مقابله با آنتی‌ویروس‌های جعلی، نرم‌افزارهای شرور امنیتی (Rogue security software)

با ورود به دوران همگانی شدن نرم‌افزارهای رایگان و کد باز (Open Source) نرم‌افزارهای امنیتی و رایگان جدیدی برای دانلود در اختیار کاربران قرار گرفتند. بازار آنتی‌ویروس‌ها از انحصار شرکت‌های بزرگی چون Kaspersky، McAfee، Symantec خارج شد و شمار بسته‌های نرم‌افزاری ضدویروس، ضدجاسوس و ضدتبلیغ به صدها و بلکه هزاران بسته رسید. اما در این میان گروهی نیز به این فکر افتادند تا با عرضه نرم‌افزارهای آنتی‌ویروس، ضدجاسوس، تمیزکننده رجیستری و پاک‌کننده حافظه Cache و با سوءاستفاده از اعتماد و عدم اطلاع کاربران، بدافزارها را در قالب آنتی‌ویروس وارد کامپیوتر کاربران نمایند. در جدول سایت ویکی‌پدیا شماری از مشهورترین آنتی‌ویروس‌های تقلبی و نرم‌افزارهای شرور امنیتی (Rogue security software) را مشاهده می‌کنید:

http://en.wikipedia.org/wiki/Rogue_security_software

اینگونه نرم‌افزارها عموما به یکی از طرق زیر وارد کامپیوتر شما می‌شوند:

- مراجعه به صفحهٔ آلوده‌ای که حاوی جاوااسکریپت یا کد اکتیو ایکس حامل برنامه شرور است.
- نصب یک افزونه آلوده و گمراه‌کننده بر روی مرورگر
- باز کردن ایمیل حاوی یک فایل اجرایی آلوده، دانلود یک محافظ صفحه نمایش آلوده
- دانلود یک فایل اجرایی ظاهرا بی‌خطر از شبکه‌های P2P، نمایش ویدئوهای نیازمند به یک کُدِک آلوده
- استفاده از یک سرویس جستجو و حذف بدافزار رایگان

اگر در گذشته بدون دقت و کنترل نام آنتی‌ویروس و برنامه‌هایی که ادعا می‌کنند، کامپیوتر شما آلوده است چنین برنامه‌هایی را نصب کرده‌اید، چاره کار استفاده از یک نرم‌افزار امنیتی مانند Microsoft Security Essentials و یا Trend Micro House Call است که به صورت همزمان قابلیت تشخیص ویروس، جاسوس و سایر بدافزارها را داشته باشد. این نرم‌افزار معمولا آخرین تهدیدهای مربوط به برنامه‌های شرور در اینترنت را وارد لیست تهدیدهای خود کرده، کامپیوتر شما را در جستجوی یک یک این تهدیدها می‌کاود.

ما در جزوه درس مربوط به مبارزه با ویروس‌ها، نرم‌افزارهای خوشنام و توانمند ویروس‌کشی نظیر Trend Micro، Avira، AVG، Comodo و چند آنتی‌ویروس دیگر را معرفی کردیم. همچنین برای خلاص شدن از تهدید جاسوس‌ها نرم‌افزار Spybot S&D به صورت مشروح معرفی شد. این نرم‌افزارها تقریبا همه آنچه را که یک کاربر عادی برای حفظ امنیت کامپیوتر ویندوز خود احتیاج دارد در اختیار او قرار می‌دهند. پس لزومی به دانلود، نصب و تست نرم‌افزارهای امنیتی بیشتر نیست چرا که آنتی‌ویروس‌ها و سایر نرم‌افزارهای شرور تقلبی امروز بیش از ۱۵ درصد موارد قابل توجه تهدید علیه امنیت سیستم‌های کامپیوتری را تشکیل می‌دهند.

مبارزه با Botnetها

بسیاری از کامپیوترهای شخصی در جهان بدون آنکه علامت خاصی از خود نشان دهند، به عنوان بخشی از شبکه‌های غول پیکر بات‌نت (Botnet) انجام وظیفه می‌کنند. بر اساس تخمین شرکت مک‌آفی بیش از ۱۲ میلیون کامپیوتر در جهان درگیر در یکی از شبکه‌های بات‌نت هستند. عضویت در بات‌نت‌ها عموما با دریافت یک ایمیل آلوده به یک اسب تروا یا نوع دیگری بدافزار آغاز می‌شود. بات‌نت‌ها در حقیقت شبکه گسترده‌ای از کامپیوترها، سرورها و بدافزارها هستند که برای مقاصد مختلفی نظیر موارد ذیل استفاده می‌شوند:

- ارسال اسپم
- جنگ‌های سایبری نظیر جنگ روسیه علیه استونی (۲۰۰۶) و گرجستان (۲۰۰۷)
- حملات DDoS به دلایل سیاسی، عقیدتی و غیره
- سرقت اطلاعات

در این اینفوگرافیک اطلاعات جالبی درباره بات‌نت‌ها خواهید یافت:

http://www.geekosystem.com/botnet-infographic/

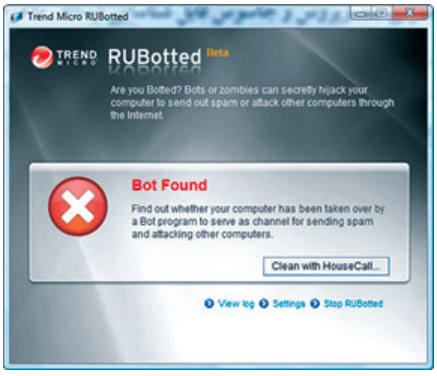
همچنین در اینجا آمار جالبی درباره بات‌نت‌ها ارائه شده است:

http://blog.trendmicro.com/big-botnet-busts/

و در اینجا کارکرد بات‌نت‌ها با روایتی داستانی همراه با تصاویر ساده و راهکارهای مقابله تشریح شده است:

http://www.thewindowsclub.com/infographic-botnets-demystyfied-and-explained

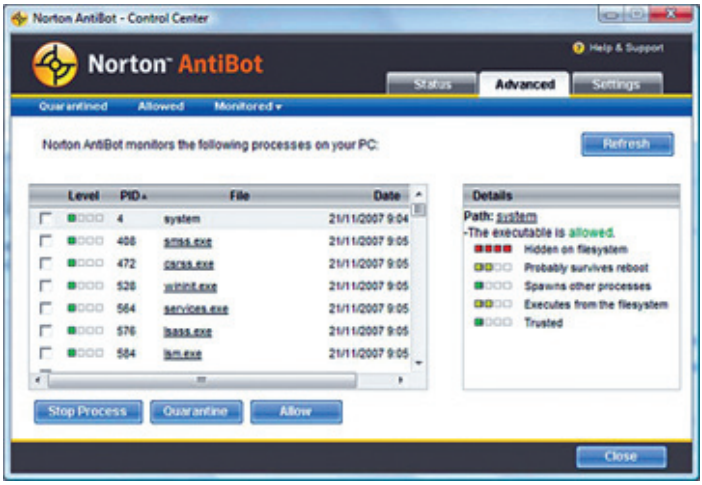
در سال ۲۰۰۹ یکی از بزرگ‌ترین بات‌نت‌ها به نام شبکه ارواح یا Ghostnet، شناسایی شد. این شبکه حاوی بیش از ۱۳۰۰ کامپیوتر در ۱۰۳ کشور مختلف بود و کامپیوترهای مراکز دیپلماتیک، مراکز سیاسی و نظامی و همچنین منتقدان دولت چین توسط کامپیوترهایی از داخل چین مورد بازرسی و دستکاری قرار گرفته بود. طراحان شبکه ارواح با روشن کردن میکروفن کامپیوترهای قربانی و همچنین دوربین وب‌کم آنها، می‌توانستند به اطلاعات فیزیکی پیرامون کامپیوتر دسترسی پیدا کنند. بسیاری از بات‌نت‌ها، با ابزارهای معمولی ضدویروس و جاسوس قابل شناسایی نیستند. ما در اینجا دو برنامه مختلف که می‌توانند از کامپیوتر شما در برابر انواعی از بات‌نت‌ها محافظت نمایند، معرفی می‌کنیم. ابزار رایگان نخست یا RUBotted از شرکت ترندمیکرو در آدرس زیر قابل دانلود است:



http://free.antivirus.com/rubotted

پس از نصب این برنامه، با ورود بدافزارهای بات‌نت‌ها به کامپیوتر شما، صفحه مقابل ظاهر خواهد شد، شما می‌توانید بلافاصله از سایت حاوی بدافزار خارج شده و حافظه Cache خود را تماما پاک کنید.

برنامه رایگان دیگر ضدبات، Norton Antibot از شرکت Symantec است که صفحه اصلی آن به این شکل است:



۶

دور زدن فیلترینگ

فیلترینگ در ایران

بر اساس تحقیقات اوپن‌نت، بیش از ۲۵ کشور مختلف در جهان هر یک به شکلی و در سطحی متفاوت مشغول سانسور اینترنت‌اند. دولت جمهوری اسلامی ایران در سطحی کم‌نظیر و با سیستمی پیچیده و چندلایه تمام تلاش خود را برای سانسور طیف بسیار گسترده‌ای از محتویات مختلف از انتشار مطالب مربوط به گروه‌های اجتماعی، موزیک و شبکه‌های اجتماعی گرفته تا مطالب و محتوای سیاسی، مذهبی، فعالیت‌های حقوق بشری و رسانه‌های خبری مستقل به کار می‌گیرد.

بر اساس یافته‌های منتج از چند تحقیق مختلف از جمله گزارشی بر اساس یافته‌های پس از انتخابات ژوئن ۲۰۰۹ که به تظاهرات و درگیری‌های وسیع انجامید، دولت ایران به طور مشخص از روش‌های زیر برای نظارت و واکاوی ترافیک اینترنتی و همچنین اعمال فیلترینگ بر سایت‌ها استفاده می‌نماید:

۱. مسدود کردن آی‌پی: روش نسبتا ساده برای مسدود کردن هر نوع ترافیک به یک آی‌پی مشخص، در بسیاری موارد کل سایت‌های میزبانی شده بر یک سرور مسدود می‌شوند. نمونه مشخص آن سرور Godaddy و یا بلاگ‌های سرویس داده شده روی Wordpress.com هستند.

۲. محدود کردن پهنای باند دسترسی: بر خلاف سخت‌افزار بازبینی و کنترل وب در کشورهایی مانند چین که بازبینی را به صورت سطحی انجام می‌دهد، بازبینی و نظارت ترافیک اینترنتی در ایران بسیار عمیق‌تر است. یعنی اجزای بسته‌های اطلاعات به صورت جزء به جزء خوانده و در مواردی در سطح عمیق یا به اختصار Deep Packet Inspection وارسی می‌شوند. مشکل این نوع وارسی، نیاز به منابع گسترده سخت‌افزاری برای انجام عمل وارسی و داده‌کاوی است و مشخصا زمانی که ترافیک اینترنتی

ایران در سطح معمولی قرار دارد (به طور مثال قبل از انتخابات ژوئن ۲۰۰۹) مشخصا سخت‌افزار وارسی داده‌ها قادر به تفکیک و وارسی ترافیک ۶ گیگابایت در ثانیه نخواهد بود. به همین منظور بلافاصله پس از شروع انتخابات، دولت ایران اقدام به محدود کردن تقریبا کامل پهنای باند کشور نمود (شیوه مشابه برمه که اساسا دسترسی کشور را به اینترنت مسدود کرد.)

۳. مسدود نمودن ترافیک بر اساس کلیدواژه یا Keyword: به‌طور مثال سایت‌ها و بلاگ‌های حاوی واژه‌های girl، woman، women و یا Moosavi، Mousavi و دیگر واژه‌های مرتبط با تظاهرات و اعتراضات پس از انتخابات فیلتر شده‌اند.

۴. طبقه‌بندی ترافیک: روشی نسبتا موثر بر مبنای طبقه‌بندی ترافیک بر اساس پروتکل‌ها یا پورت‌های انتقال داده است، به طور مثال می‌توان پهنای باند ترافیک داده به پورت ۸۰ و پروتکل TCP را محدود کرد و این به معنای محدودیت پهنای باند برای مرور صفحات HTTP است. همین عمل را می‌توان برای پروتکل‌های دیگر نظیر FTP نیز انجام داد. ارتباطات VOIP و یا نرم‌افزارهایی نظیر Skype را عملا از کار انداخت. بر اساس اطلاعات دریافتی در گزارش مورگن سنهاوزر، این پروتکل‌ها و سرویس‌های در ایران به صورت محسوسی محدود شده‌اند: HTTPS و SSH.

۵. بازرسی سحطی بسته‌های داده (Shallow Packet Inspection): بر خلاف روش بازرسی عمیق بسته‌های داده (DPI) که مختصرا توضیح داده شد، هزینه سخت‌افزاری و نیروی انسانی گزافی را به دولت ایران تحمیل می‌نماید. روش SPI، تنها به آزمایش سربرگ هر بسته پرداخته و با بازخوانی ارقام سربرگ نظیر طول داده و یا پروتکل انتقال، محتوای نسبی بسته حدس زده می‌شوند و سپس داده‌های مشکوک برای بازبینی دقیق‌تر تحویل روش چهار یا طبقه‌بندی ترافیک می‌شوند. این روش مورد استفاده‌ترین روش در بازرسی داده در ایران در زمان حاضر است.

۶. روش بازرسی اثر انگشت بسته‌ها (Fingerprint Inspection): در این روش سربرگ بسته‌ها چندان مورد بازرسی قرار نمی‌گیرند، چرا که می‌توانند حاوی اطلاعات گمراه‌کننده باشند. در این روش مشخصات و ویژگی‌های بسته مورد توجه قرار می‌گیرد و با توجه به این ویژگی‌ها مثلا طول بسته، سعی می‌شود تا محتوای بسته حدس زده شود. این روش روشی متکی به سخت‌افزار نسبتا پرقدرت است و به نظر می‌رسد ایران در حال آماده‌سازی بستر سخت‌افزاری لازم برای استفاده از این روش باشد.

۷. بازرسی عمیق بسته‌ها یا Deep Packet Inspection که قبلا مختصرا توضیح داده شد، روشی بر پایه مطالعه دقیق و جزء به جزء محتویات بسته است؛ حتی محتویات بسته‌های کدگذاری‌شده یا encrypted را نیز می‌توان با این روش شناسایی کرد. در حال حاضر میزان استفاده ایران از این روش چندان روشن نیست، اما به دلیل دشواری‌های تکنیکی این روش برای سیستم نظارت ایران، به نظر می‌رسد از این روش استفاده حداقلی می‌شود.

چه چیز فیلتر می‌شود؟

- بیت تورنت و بسیاری از آدرس peerهای اشتراک داده و یا سرور حاوی آدرس peerها
- سایت‌های خبررسانی خارجی و سایت‌های اصلاح‌طلب، مستقل و منتقد فعال در خبررسانی داخلی

• بلاگ‌ها، بسیاری از بلاگ‌های منعکس‌کننده اخبار، تصاویر و ویدئوهای اعتراضات و یا همان‌طور که گفته شده سایت‌های گلوبال سرویس‌دهنده بلاگ نظیر Wordpress و یا Blogspot. همچنین بلاگ‌های حاوی مطالب غیراخلاقی از نظر دولت ایران و بلاگ‌های ارائه‌کننده ابزارهایی نظیر فیلترشکن‌ها.

• سایت‌های سیاسی اصلاح طلب، مستقل و منتقد و حتی محافظه‌کار میانه‌رو

• سایت‌های ارائه‌کننده ابزارهای فیلترشکن و دیگر ابزارها و امکانات عبور از فیلتر

• پروکسی‌سرورها، پروکسی‌سرورها بلافاصله پس از معرفی یک روزنه برای عبور از سد سانسور آنلاین، مسدود می‌شوند.

استفاده از فیدهای RSS برای دورزدن فیلترها

امروزه تقریبا تمام سایت‌های و بلاگ‌های فارسی و غیرفارسی امکان اشتراک فید آر.اس.اس را عرضه می‌کنند. شما می‌توانید قبل از فیلتر شدن یک بلاگ یا سایت خبری، فید آر.اس.اس آن را مشترک شوید و یا با استفاده از ابزارهای دیگر دور زدن فیلتر این‌کار را یک بار انجام دهید. چرا که پس از اشتراک (Subscribe) به فید در محیطی مانند Google Reader یا هر فیدخوان دیگر، تمامی مطالب سایت به صورت اتوماتیک در اختیار نرم‌افزار فیدخوان شما قرار خواهد گرفت.

برای دریافت و مطالعه فیدها نرم‌افزارهای زیادی وجود دارد. اما استفاده از فیدخوان گوگل یا یاهو برای دسترسی و اشتراک فیدهای آر.اس.اس و اتم، توصیه می‌شود. برای اشتراک کافی‌ست زمانی که در اکانت گوگل خود حضور دارید دکمه بالای صفحه یا اشتراک فید آر.اس.اس را فشار دهید. فید مورد نظر به صورت اتوماتیک به خوراک‌خوان گوگل شما – یا به قول کاربران ایرانی گودر – اضافه خواهد شد. برای دسترسی به همه فیدهای خود کافی‌ست وارد آدرس گودر خود شوید:

http://www.google.com/reader

متاسفانه در ماههای گذشته شرکت گوگل تغییراتی بر سرویس گودر اعمال کرده است که کار را برای کاربران ایرانی که این امکان را برای خواندن خوراک – فید سایت‌های سانسور شده استفاده می‌کردند، مشکل نموده است. گوگل در موارد مشابه همواره نشان داده است که از آزادی بیان و تبادل اطلاعات دفاع می‌کند و برخی بر این باورند که گودر به درخواست‌های پردامنه ده‌ها هزار کاربر ایرانی به شکلی قابل قبول پاسخ خواهد داد.

در حال حاضر بسیاری از کاربران ایرانی روش‌های جایگزینی برای بازگشت به گودر پیشنهاد کرده‌اند، یکی از این روش‌ها استفاده از افزونه‌های مرورگرهای کروم و فایرفاکس است. در مورد کروم می‌توانید این افزونه Reader Sharer را استفاده نمائید:

https://chrome.google.com/webstore/detail/gmgmcmhmodidojodfoekpbjnejlhcbpb

برای فایر فاکس هم می‌توانید از افزونه Reader Sharer Monkey استفاده کنید:

http://userscripts.org/scripts/show/117034

به خاطر داشته باشید برای فایرفاکس باید افزونه Greasemonkey را قبلا نصب کرده باشید.

استفاده از VPNها برای عبور از فیلتر

در ماه‌های گذشته دولت ایران نبرد بی‌سابقه‌ای را علیه VPNها یا شبکه‌های خصوصی مجازی که توسط میلیون‌ها ایرانی برای عبور از سد فیلترها به کار برده می‌شدند، آغاز کرد. مخابرات با مسدود نمودن پورت‌ها یا گذرگاه‌های ارتباطی، کاربرانی را که از VPN L2tp و همچنین PPTP استفاده می‌نمودند را دچار مشکل کرد. چارهٔ باقی مانده برای کاربران استفاده از IPsec بود، در مرحله جدید فروشندگان وی‌پی‌ان وعده می‌دهند سرورهای جدید ایشان همه پروتکل‌های ویندوز برای وی‌پی‌ان را پشتیبانی می‌کند: PPTP-L2TP/IPSEC-SSTP-SSH-SSL-socks5.

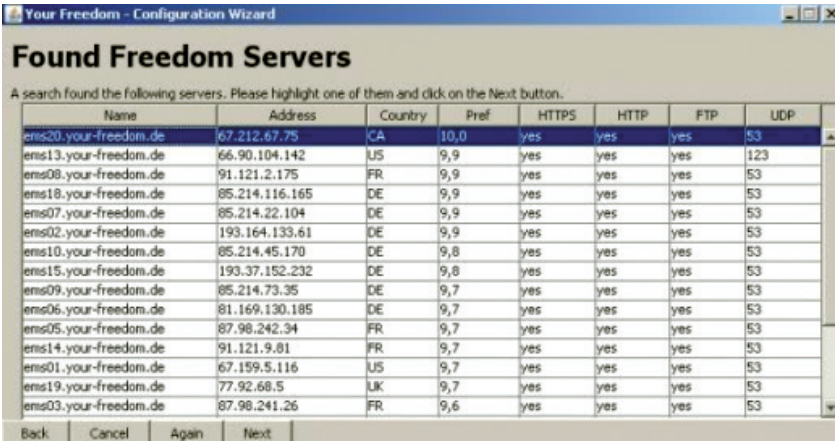
از طریق لینک زیر می‌توانید توضیحات مفصلی پیرامون ۱۰ سرویس‌دهنده امن VPN در جهان را بخوانید. البته هیچ یک از این سرویس‌ها رایگان نیستند، اما با توجه به اقداماتی که دولت ایران برای کنترل و سرکوب دیجیتال شهروندان جهان مجازی انجام می‌دهد، استفاده از سرویس‌هایی که بیشترین توجه را به امنیت و حریم خصوصی کاربران دارند، از اهمیت خاصی برخوردار است:

http://www.dw.de/dw/article/0,,15394437,00.html

استفاده از امکانات Your-freedom برای عبور از فیلتر

Your-freedom در آدرس http://www.Your-freedom.net/ ارائه می‌شود، اگرچه بهتر است همواره از حالت https:// این سایت استفاده شود.

در سایت Your-freedom، راهنمای کاملی برای دانلود و استفاده از Your-freedom ارائه شده است. برای کاربران عادی، پس از نصب Your-freedom این برنامه به دنبال سرورهای آزاد Your-freedom خواهد گشت:



برنامه Your-freedom امکان استفاده این نرم‌افزار با OpenVpn را نیز فراهم آورده است. برای مطالعه کامل این روند از آدرس منبع استفاده نمائید:

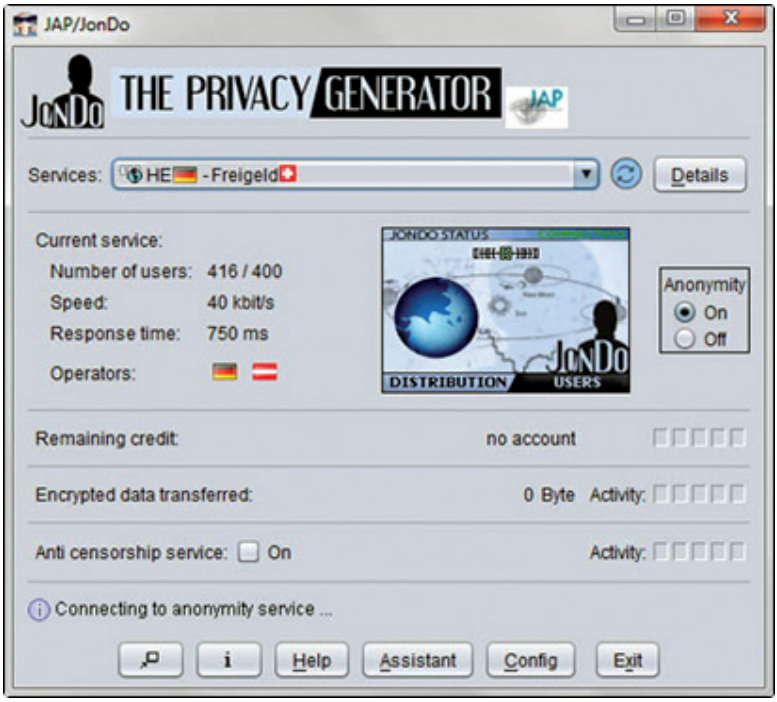
http://www.your-freedom.net/index.php?id=175

اگر می‌خواهید توضیحات بیشتری درباره Your Freedom و سایفون به فارسی بخوانید به اینجا مراجعه کنید:

https://www.azadcyber.info/articles/679

JonDo

برنامه دیگری که تقریبا کارکردی شبیه به Your Freedom دارد، JonDo است که عموما از طریق سرورهای واسطه آلمانی امکان عبور از سد فیلترینگ را فراهم می‌کند.



برای کسب اطلاعات بیشتر درباره این برنامه می‌توانید به اینجا مراجعه کنید:

https://www.azadcyber.info/articles/924

افزونه‌های فایرفاکس

بسیاری از کاربران ایرانی همه ماه‌های گذشته را به تلاش برای یافتن راه‌های موثری به منظور دورزدن فیلترها گذراندند، نتیجه این تلاش‌ها رواج افزونه‌های متعددی برای فایرفاکس بود که در مواردی به دورزدن فیلترها کمک می‌کرد.

یکی از این افزونه‌ها در لینک زیر معرفی می‌شود:

https://addons.mozilla.org/en-US/firefox/addon/access-freeneti/

ظهور مجدد سایفون (Psiphon)

با انتشار Psiphon3 و مشکلاتی که برای VPNها و سرعت سرورهای اولتراسرف و فری‌گیت به وجود آمده بود، بسیاری از کاربران مجددا بخت خود را با استفاده از Psiphon3 آزمودند.

از طریق لینک زیر می‌توانید فایل اجرایی Psiphon را دانلود کنید:

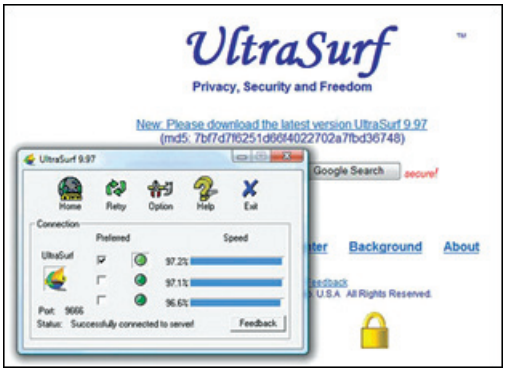
https://s3.amazonaws.com/f58p-mqce-k1yj/psiphon3.exe

پس از نصب Psiphone ارتباط با سرور به صورت خودکار برقرار می‌شود و با سبز شدن آیکون، شما استفاده از سایفون را آغاز می‌نمائید.

اولتراسرف از Ultrareach

اولتراسرف از اولتراریچ، یک وسیله پرطرفدار برای دور زدن سانسورهای اینترنتی خصوصا در جمهوری خلق چین است. برای استفاده از این سرویس باید نرم‌افزار اولتراسرف را از سایت شرکت سازنده برنامه دانلود و نصب نمود:

http://ultrasurf.us/



اگر از مرورگر فایرفاکس استفاده می‌کنید، باید افزونه اولتراسرف برای فایرفاکس را نیز دانلود کنید.

قابلیت‌های اولترا سرف به صورت مختصر عبارتند از:

سادگی و حجم کم این برنامه، بلافاصله پس از دانلود فایل کم‌حجم برنامه و اجرای آن، سه جزء برنامه اولتراسرف ظاهر می‌شوند؛

علامت قفل طلایی کنار صفحه که با آن می‌توانید از برنامه خارج و یا به صفحه تنظیم برنامه بروید. دقت کنید که در صفحه تنظیمات برنامه امکانات ویژه‌ای چون پاک کردن حافظه اینترنت اکسپلورر شما پس از خروج از اولتراسرف هم پیش‌بینی شده است؛ حتما این امکانات را فعال کنید.

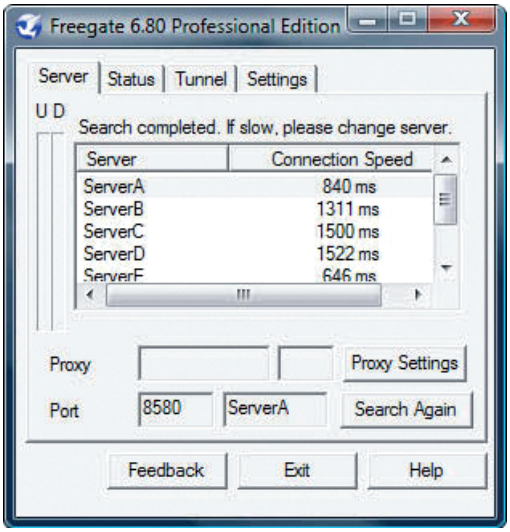
یک نکته مهم در استفاده از اولتراسرف: خارج شدن ناگهانی از این ابزار ممکن است دسترسی شما به اینترنت را محدود کرده یا کلا مختل سازد، چارهٔ این کار ساده است؛ بایستی مجددا به اولتراسرف وارد و سپس در صورت تمایل به خروج، از دکمه سمت راست ماوس بر روی قفل طلایی استفاده کرده و گزینه خروج یا Exit را انتخاب نمائید.

فری‌گیت (Freegate)

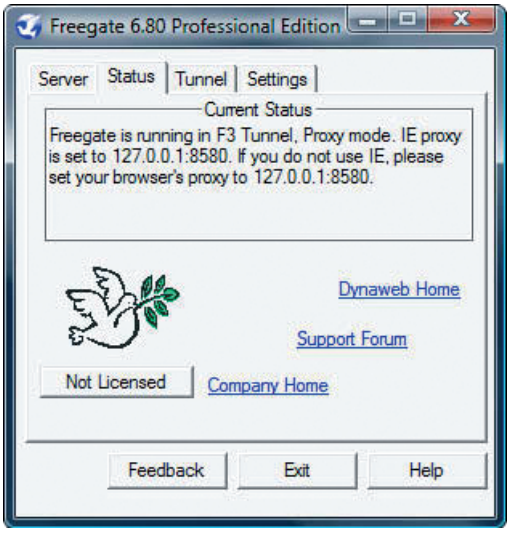
فری گیت ابزار تونل موثر دیگری برای دورزدن سانسورهای دولتی است که در ابتدا برای کمک به کاربران اینترنت در جمهوری خلق چین طراحی شده است. برای دانلود نرم‌افزار فری‌گیت می‌توانید از سایت‌های بزرگ دانلود نظیر Download.com استفاده نمائید و تنها کافیست کلمه Freegate را در محل جستجو تایپ کنید.

پس از دانلود و اجرای فایل اجرائی برنامهٔ فری‌گیت که در حال حاضر به شکل fg680f.exe است، پنجره اینترنت اکسپلورر شما به صورت خودکار باز شده و صفحه زیر به نمایش درخواهد آمد:

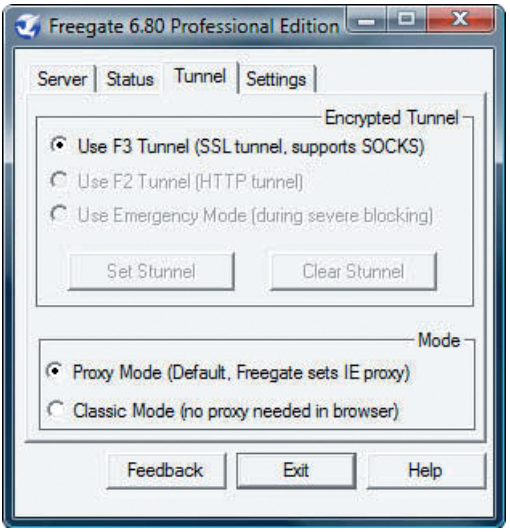
همچنین منوی برنامه فری‌گیت نیز در شکل زیر ظاهر خواهد شد و پس از جستجو، لیست سرورهای در دسترس را به نمایش خواهد گذاشت:



شما با ورود به قسمت وضعیت یا Status می‌توانید از اجرای کامل فری گیت، تونل بودن ارتباطات خود از طریق اینترنت اکسپلورر اطمینان حاصل نمایید. توجه کنید که اگر مایل به استفاده از مرورگر دیگری مثلا اپرا یا فایرفاکس هستید کافی‌ست آدرس پروکسی در قسمت تنظیمات مرورگر خود را به آدرس پیشنهادی فری‌گیت، در مثال فعلی (127.0.0.1:8580) تغییر دهید. قسمت آخر این آدرس، حاوی مشخصات درگاه یا پورت مورد استفاده فری‌گیت است که می‌بایست در مرورگرهای غیر اکسپلورر تنظیم شود.

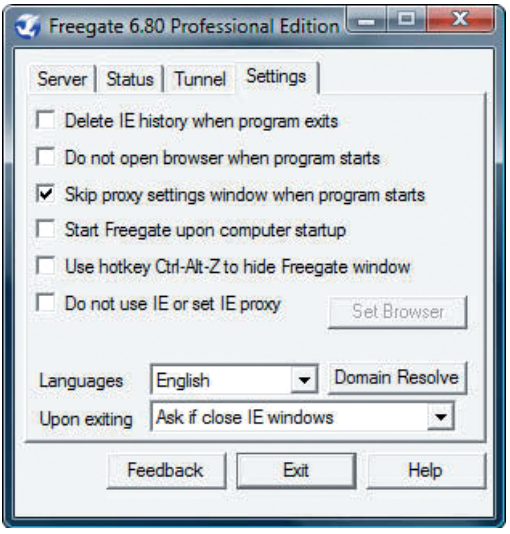


قسمت بعدی یا Tunnel، نمایانگر تنظیمات تونل فری‌گیت است. استفاده از تونل موسوم به F3 با پروتکل امن و کدگذاری شده SSL قویا توصیه می‌شود:



قسمت بعدی Setting یا تنظیمات فری‌گیت برای مرورگر شماست. در این بخش می‌توانید از فری گیت بخواهید پس از خروج از روند تونل کردن اطلاعات، حافظه مرورگر شما را به طور کامل پاک کند و یا به طور خودکار پس از روشن کردن کامپیوتر فری‌گیت را اجرا نماید.

همچنین اگر به دلایلی قصد استفاده از اینترنت اکسپلورر و به تبع آن علاقه‌ای به تغییر پروکسی و پورت اینترنت اکسپلورر خود ندارید، می‌توانید با علامت‌گذاری در قسمت مربوطه تغییرات مورد نظر خود را اعمال نمایید.



Gpass

جی پاس نرم‌افزار نسبتا پیچیده‌ای برای دور زدن سانسورهاست که قابلیت‌های گسترده‌ای دارد. به صورت خیلی مختصر جی‌پاس بسته‌های اطلاعات شما در هنگام استفاده از اینترنت را قبل از انتقال، فشرده و کدگذاری امن می‌نماید. مزیت دیگر جی‌پاس امکان رمزگذاری برنامه‌های مختلفی نظیر تور و اسکایپ در آن است در حقیقت جی‌پاس بیشتر ارتباطات کامپیوتر شما را رمزگزاری و مخفی می‌کند، تنها استثنای عدم کدگذاری جی‌پاس ارتباطات به شیوه Socks Direct است.

شما می‌توانید برنامه قابل حمل و سبک جی‌پاس را از آدرس زیر دانلود نمایید:

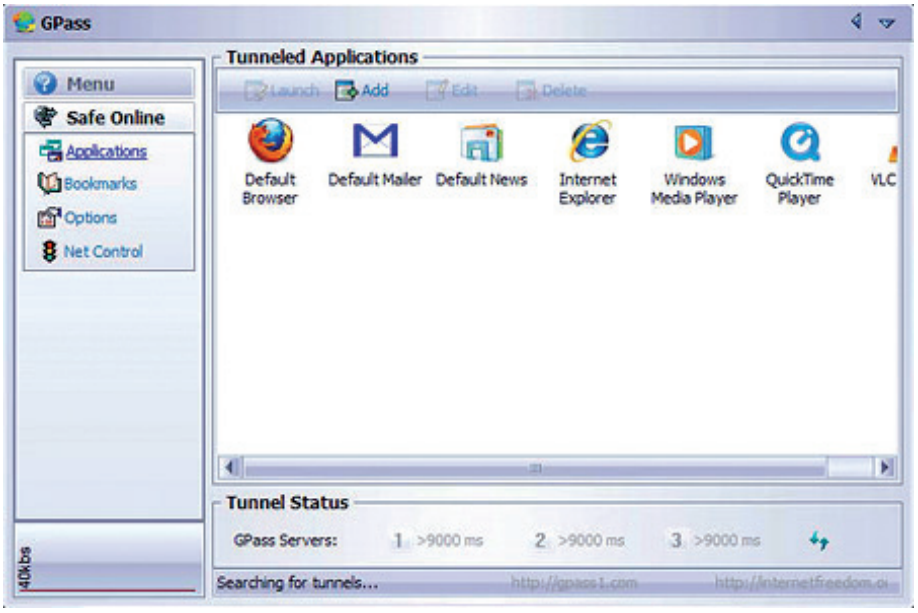
http://gpass1.com

کتاب راهنمای جی‌پاس نیز به زبان فارسی در آدرس زیر موجود است:

http://gpass1.com/help-fa

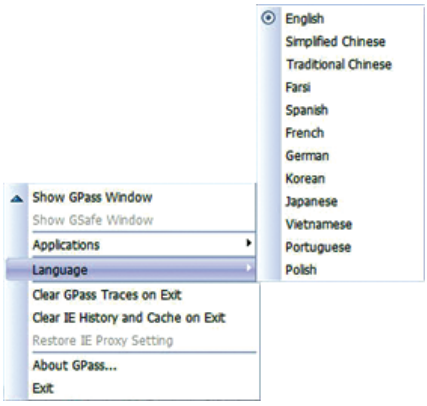
در صورت فیلتربودن این سایت می‌تواند جی‌پاس را از دیگر سایت‌های دانلود، دانلود کنید. اما مراقب باشید که این سایت‌ها از جمله سایت‌های معتبر دانلود نظیر Download.com باشند. نسخه‌های تقلبی نرم‌افزارهای تونل به وفور در اینترنت به چشم می‌خورند و قادرند کامپیوتر را با مشکلات جدی امنیتی مواجه سازند.

پس از دانلود و اجرای جی‌پاس پنجره زیر ظاهر خواهد شد و جی‌پاس بلافاصله اینترنت اکسپلورر شما را برای دور زدن سانسور پیکربندی یا تنظیم خواهد کرد:



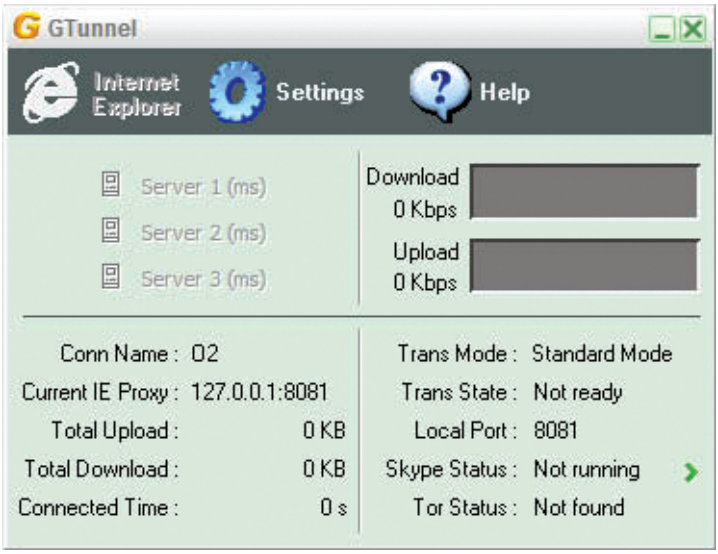
توجه کنید که با کلیک سمت راست روی گردونه خاکستری رنگ جی‌پاس، منویی باز خواهد شد که از طریق آن می‌توانید جی‌پاس را تنظیم نمائید.

اضافه بر امکان انتخاب زبان مثلا فارسی، بهتر است از جی‌پاس بخواهید پس از خروج از حالت مرورگری امن، حافظه اکسپلورر شما را پاک کند.



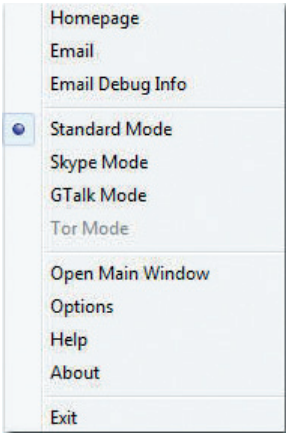
Gtunnel

جی‌تونل، برنامه تحت ویندوز دیگری برای عبور از فیلترهاست. جی‌تونل قادر به پنهان کردن آدرس آی‌پی کاربر و همچنین رمزگذاری ترافیک میان کامپیوتر کاربر و سرورهای جی‌تونل است. فایل نسبتا کوچک جی‌تونل را می‌توانید از آدرس http://gardennetworks.org/download دانلود کنید. پس از اجرا پنجره زیر ظاهر خواهد شد:



جی تونل نیز مانند نرم‌افزارهای دیگر تونلینگ، قابلیت تنظیم با فشردن دکمه سمت راست ماوس

بر روی علامت G پایین صفحه را دارد. در اینجا علاوه بر تنظیم مربوط به پاک کردن حافظه مرورگر می‌توانید جی‌تونل را برای استفاده در دیگر ارتباطات کامپیوتر خود نظیر ایمیل تنظیم نمائید.



محافظت از هویت با استفاده از تور (TOR)

تور از ابزارهای محافظت از هویت و ناشناس ماندن شما به هنگام مرور اینترنت است. تور از شبکه‌ای از کاربران و کامپیوترهای داوطلب ایجاد شده است که با اشتراک نرم‌افزار تور، ترافیک را از دستگاهی به دستگاه دیگر هدایت می‌کنند به شکلی که شناسایی مبداء ترافیک بسیار دشوار خواهد بود.

در صورتی که قصد دارید تور را بر روی سیستم عامل ویندوز خود نصب کنید باید همه اجزاء بسته تور یعنی Polipo، Torbutton، Vidalia، Tor را دانلود کنید. مجموعه فشرده این بسته در آدرس زیر قابل دسترسی است:

http://www.torproject.org/docs/tor-doc-windows.html.en

در هنگام استفاده از تور و قالب نرم‌افزارهای حفظ هویت، رعایت نکات زیر بسیار ضروری است:

• تور ناشناسی شما را فقط در برنامه‌هایی محافظت می‌کند که برای استفاده از تور تنظیم شده باشند. تصور نکنید با نصب تور همه ترافیک اطلاعات شما، محرمانه و محافظت می‌شود. مثلا استفاده امن از فایرفاکس تنها با دانلود افزونه Torbutton از اجزای بسته نرم‌افزاری تور برای ویندوز ممکن است.

• توربانت، معمولا همه روش‌های مختلف تشخیص آی‌پی شما را بلوکه می‌کند، از پی‌دی‌اف‌خوان مرورگر گرفته تا پلاگین‌های اکتیو ایکس، جاوا، فلش، QuickTime، RealPlayer و غیره. یک مثال کامل بلوکه کردن، یوتیوب است. اگر بر استفاده از یوتیوب اصرار دارید. می‌توانید با ایجاد استثنا در توربانت این کار را انجام دهید. اما توجه داشته باشید که ایجاد استثنا به منزله گشودن دریچه‌ای برای کاهش امنیت است.

• تور تنها ترافیک میان کامپیوتر شما و کامپیوترهای شبکه تور را رمزگذاری می‌کند. ترافیک نهایی میان شبکه و کامپیوتر مقصد رمزگذاری نمی‌شود. اگر قصد ارسال اطلاعات محرمانه و حساس را دارید

از پروتکل‌های امنی چون اس‌اس‌ال استفاده کنید.

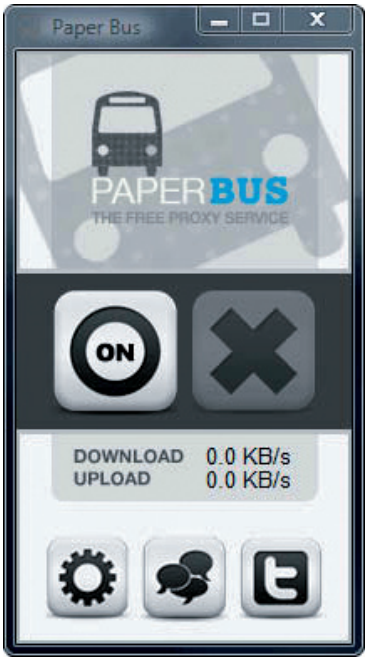
• مراقب کوکی‌ها باشید، تور از آغاز اجرا، عملکرد کوکی‌هایی که قصد باز شدن روی کامپیوتر شما را دارند کنترل می‌کند، اما کوکی‌هایی که قبل از اجرای تور روی کامپیوتر شما نصب شده‌اند هنوز می‌توانند یک خطر بالقوه باشند. Torculler می‌تواند شما را برای مدیریت کوکی‌های ناخواسته کمک کند.

• تور کامپیوتر شما را از حمله‌های ورودی محافظت می‌کند، اما توجه داشته باشید که کامپیوترهای آلوده‌ای می‌توانند عضو داوطلب شبکه تور شده و برای شما بدافزار ارسال نمایند. در هنگام دانلود برنامه از خلال تور دقت کنید.

Paperbus

Paperbus یک سرویس رایگان پروکسی است که توسط کابران در کشورهای مختلف مورد استفاده قرار می‌گیرد. نرم‌افزار Paperbus حدود ۷ مگابایت حجم دارد و از آدرس زیر قابل دانلود است:

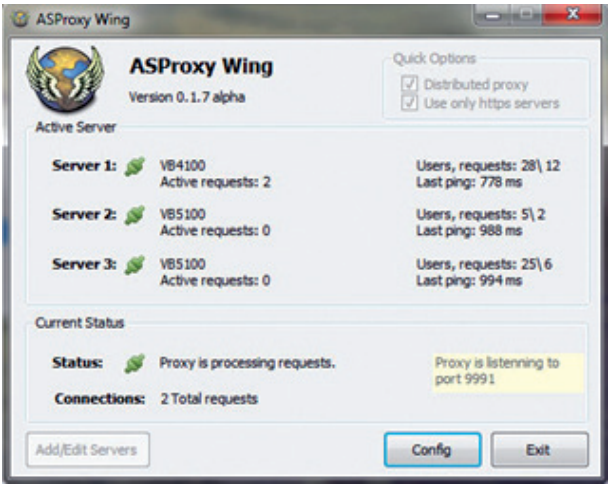
http://www.paperb.us/#download



ویژگی جالب Paperbus تغییر اتوماتیک تنظیمات اینترنت اکسپلورر، گوگل کروم و فایرفاکس برای استفاده ناشناس و امن از اینترنت است. در منوهای نرم‌افزار Paperbus از دو کشور ایران و چین نام برده شده است.

فیلترشکن پرسرعت ASProxy Wing

این فیلترشکن چندان در میان کاربران ایرانی شناخته شده نیست، اما نسبت به سایر گزینه‌ها سرعت بالاتر و کارآیی بهتری دارد.

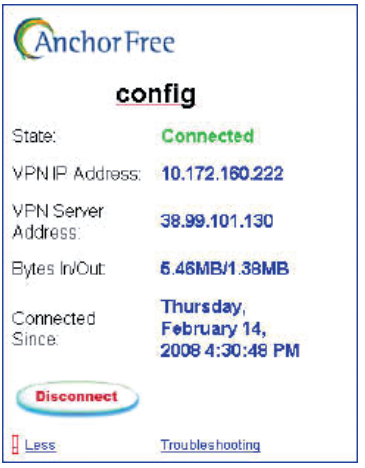


این برنامه بسیار کم‌حجم (۳۰۰ کیلوبایت) و کاربرپسند است. راهنمای کامل نصب و استفاده از این فیلترشکن را می‌توانید از اینجا ببینید:

https://www.azadcyber.info/articles/1131

هات‌اسپات‌شیلد (Hotspotshield)

محافظ هات‌اسپات، نرم‌افزاری است که در سراسر جهان، خصوصا به هنگام استفاده از شبکه‌های وایرلس عمومی استفاده می‌شود. هات‌اسپات‌شیلد، اطلاعات کاربران را به صورت رمزگذاری شده از خلال شبکه وی‌پی‌ان به سرورهای خود هدایت کرده و ترافیک بازگشتی را مجددا بدون آنکه کامپیوتر و یا شبکه میزبان قابلیت ردیابی سیستم درخواست اولیه کاربر را داشته باشند، باز می‌گرداند.



در استفاده از هات‌اسپات هویت کاربر به صورت ناشناس باقی می‌ماند. این نرم‌افزار در آدرس زیر قابل دانلود است:

http://hotspotshield.com

راهنمای کامل (اسلاید شو) نصب و استفاده از هات‌اسپات‌شیلد را می‌توانید از اینجا مشاهده کنید:

https://www.azadcyber.info/articles/2340

۷

امنیت برای شبکه‌های اجتماعی[1]

آمارهایی برای آشنایی با وضعیت امنیتی فیس‌بوک

- چهار میلیون کاربر فیس‌بوک، روزانه اسپم دریافت می‌کنند.
- حدود ۲۰ درصد فیدهای خبری فیس‌بوک حامل بدافزار هستند.
- روزانه اکانت ۶۰۰ هزار کاربر فیس‌بوک دزدیده می‌شود.

1. Social networking

مثالی برای توصیف تهدیدها در شبکه‌های اجتماعی

تهدید امنیتی بسیار ساده: سامان استاتوس خود در فیس‌بوک را به شکل زیر تغییر می‌دهد:

Its finally holiday time again! I'm on my way to Palm Springs...

از دانشجویان سوال کنید چگونه این استاتوس ساده می‌تواند یک تهدید جدی امنیتی باشد؟

۱۵ درصد از شهروندان ایالات متحده، در شبکه‌های اجتماعی می‌نویسند که در خانه حضور ندارند و ۳۵ درصد از جوانان ۱۸ تا ۳۴ سال موقعیت جغرافیایی خود را منتشر می‌کنند.

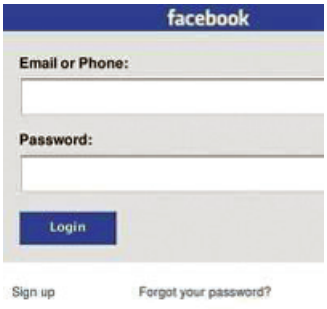
سارقان منازل از استاتوس افرادی که به مسافرت رفته‌اند سوء استفاده می‌کنند، آنان با امکاناتی نظیر Google Street View می‌توانند جوانب منزل و موانع اطراف آن را مطالعه کنند.

نکاتی ساده و ابتدایی برای کاربران عادی

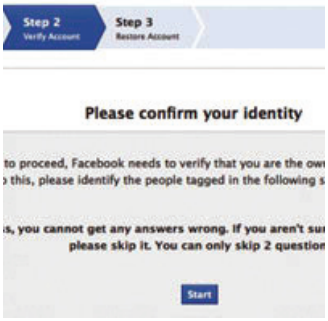
- از پسورد قوی برای فیس‌بوک استفاده کنید.
- تقاضای دوستی افراد ناشناس را به هیچ وجه نپذیرید.
- هر مورد به اشتراک گذاشته شده توسط دوستان خود را به سادگی کلیک نکنید.
- تحت هر شرایطی از https استفاده کنید.
- از کافی‌نت‌ها یا تلفن‌ها و تبلت‌ها و لپ‌تاپ دیگران وارد فیس‌بوک نشوید.
- حتما پس از استفاده Log out کنید.
- Temporary fileهای مرورگر خود را دائما پاک کنید.
- اگر مسافر کشوری مانند ایران هستید، توجه کنید که در حال حاضر ممکن است همه عکس‌های فیس‌بوک شما در اختیار دولت ایران قرار داشته باشد. آیا هنوز قصد سفر دارید؟
- روی لینک‌های مشکوک مثل «شما برنده یک آیفون هستید» کلیک نکنید.
- در صفحات امنیت فیس‌بوک عضو شوید: facebook.com/security

ابزارهای امنیتی فیس‌بوک

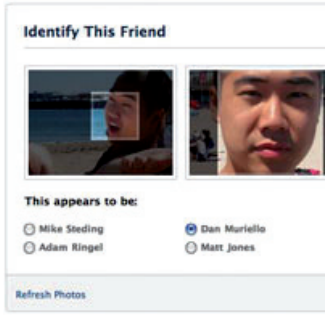
برخی از اساسی‌ترین امکانات امنیتی فیس‌بوک از قرار ذیل است:



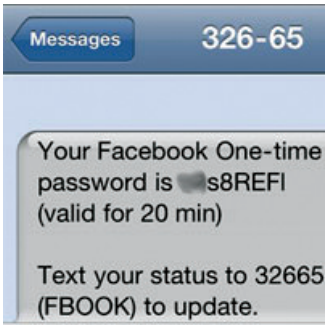
Login: برای ورود به فیس‌بوک نام کاربری و پسورد خود را وارد می‌کنید. ارتباط SSL برقرار می‌شود.



ID verification: (انتخابی؛ توصیه می‌شود فعال کنید) در اینجا می‌توانید سوالات امنیتی خود و شماره تلفنی را تعریف کنید، فیس‌بوک هربار برای شما کدی را می‌فرستد که با آن می‌توانید وارد اکانت شوید.

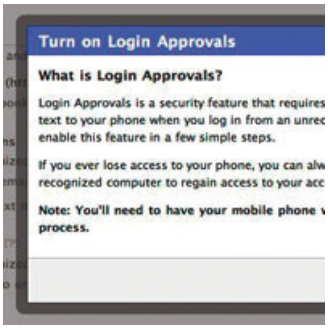


شناسایی اجتماعی یا Social Authentication: اگر مشکل خاصی در ورود شما وجود داشته باشد، مثلا امروز صبح از جایی هزاران کیلومتر دورتر لاگین کرده باشید، فیس‌بوک از شما اطلاعاتی را راجع به تاریخ تولد و یا حتی دوستان شما خواهد پرسید تا از هویت واقعی شما مطمئن شود.

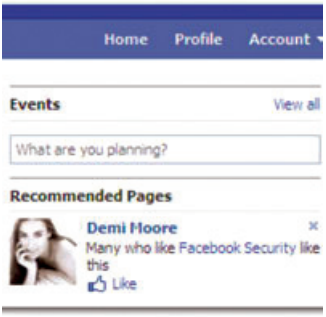


One Time Passwords: اگر شماره موبایل خود را قبلا در فیس‌بوک وارد کرده‌اید، فیس‌بوک برای شما یک پسورد یک‌بارمصرف تکست می‌کند تا از آن برای ورود به اکانت خود استفاده کنید.

اینجا درباره افزایش امنیت در فیس‌بوک با پسوردهای یک‌بارمصرف بیشتر بخوانید:
http://www.dw.de/dw/article/0,,6116519,00.html

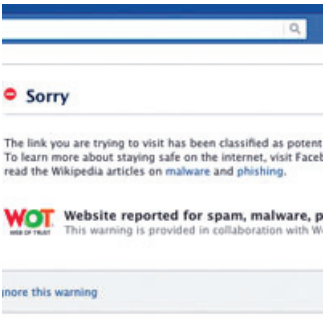


Login Approvals: (انتخابی؛ توصیه می‌شود فعال کنید) فرض کنید دفعه گذشته از کامپیوتر خانه به فیس‌بوک رفته‌اید، این بار اگر تلاش کنید از کامپیوتر جدیدی مثلا در محل کار وارد فیس‌بوک شوید. فیس‌بوک درباره کامپیوتر جدید از شما سوال می‌کند. همچنین در اکانت شما پیامی نمایش داده می‌شود مبنی بر اینکه شما با یک دستگاه جدید وارد فیس‌بوک شده‌اید.



Session Classifier: فیس‌بوک مشخصات هر ورود و خروج شما را به دقت کنترل می‌کند. این داده‌ها بررسی می‌شوند تا مثلا کاربری که صبح از سیدنی وارد فیس‌بوک شده است، قبل از نهار این بار از لندن وارد فیس‌بوک نشود.

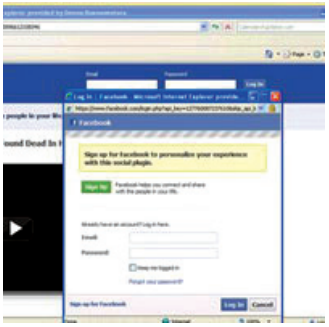
User Action Classifier: فیس‌بوک رفتار شما را زیر نظر داشته و تحلیل می‌کند. مثلا کاربری که وارد یک گروه شده است و برای ۱۵۰ کاربر جنس مخالف یک پیام مشخص را ارسال کند و یا کاربری که قصد تبلیغ و فروش اجناس روی فیس‌بوک را داشته باشد به سرعت شناسایی و دسترسی آنان محدود می‌شود.



Link Scanner: لینک‌هایی که روی فیس‌بوک ارسال می‌شود، هر روز کاملا چک می‌شوند تا کاربران را به سوی سایت‌های حاوی بدافزار هدایت نکنند.

Photo DNA: فیس‌بوک از سیستم DNA تصویری استفاده می‌کند. این سیستم قادر است میلیون‌ها تصویری را که روزانه به فیس‌بوک آپلود می‌شوند. یک به یک تحلیل کرده و مانع از آپلود تصویرهای غیرقانونی و نامتناسب با قوانین فیس‌بوک شود.

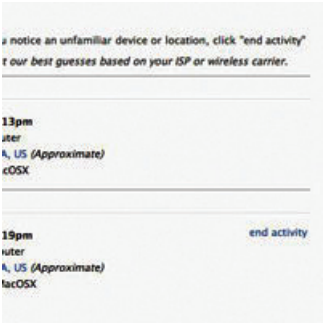
Self XSS: فیس‌بوک با کنترل کامل بخش آدرس مرورگر مانع از فعالیت اسکریپ‌هایی می‌شود که به صورت خودکار قصد انجام عملیات خاصی نظیر تغییر استاتوس یا ارسال اسپم را دارند.



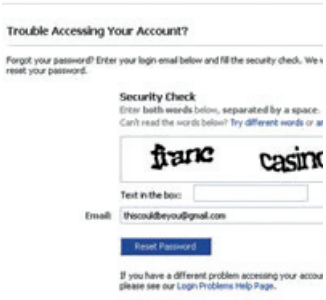
Clickjacking Domain Reputation System: فیس‌بوک مانع از پدیدار شدن خودکار یک سایت پس از کلیک کردن کاربر روی لینکی که صرفا برای دزدیدن کلیک ارسال شده می‌شود.

Application Classifier: فیس‌بوک رفتار اپلیکیشن‌ها یا برنامه‌های کاربردی را کنترل می‌کند و دائما آنان را مورد تست‌های مختلفی قرار می‌دهد تا اطمینان حاصل کند خطری برای کاربران به حساب نمی‌آیند.

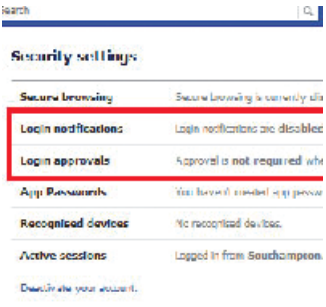
Suspected Hacking: اگر به هنگام کار با فیس‌بوک تشخیص دهید فرد یا دستگاه دیگری با اکانت شما اکتیو است، می‌توانید از اکانت خارج و تمام پسوردها را عوض کنید.



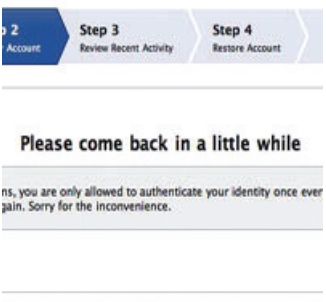
Remote Logout: فرض کنید از کامپیوتر شخص دیگری وارد فیس‌بوک خود شده‌اید و فراموش کرده‌اید LogOut کنید. به راحتی می‌توانید وارد اکانت خود شوید و در لیست فعالیت‌ها، کامپیوتر اکتیو را پیدا کنید و از راه دور فیس‌بوک را در آن کامپیوتر یا تلفن هوشمند ببندید.



Guardian Angels: اطلاعات اکانت شما در صورت گم کردن پسورد یا مشکلات دیگر می‌تواند برای دوستان نزدیک شما ارسال شود.



Login Notifications: دستگاه‌ها، کامپیوتر و یا تلفن جدیدی که به فیس‌بوک شما متصل شده باشد، در لیست اعلانات یا notifications شما نمایش داده می‌شود.



Roadblock: اگر اکانت شما رفتاری غیرعادی خصوصا در زمینه ارسال بدافزار انجام دهد. دسترسی شما برای مدتی به فیس‌بوک محدود خواهد شد تا این موارد جزء به جزء مورد بررسی قرار گیرند.

با نگاهی به این اینفوگرافیک، می‌توانید اطلاعات آماری جالبی درباره حملات فیس‌بوکی در سال ۲۰۱۱ به‌دست آورید:

http://blog.commtouch.com/cafe/web-security/infographic-facebook-attacks-in-2011/

فرصت‌های نوین، تهدیدهای نوین

فعالان مدنی در سراسر جهان با استفاده از توانایی‌های بی‌نظیر شبکه‌های اجتماعی در بسیج کنشگران، تغییرات بنیادین بسیاری ایجاد کرده‌اند. در تهران (۲۰۰۹)، تونس (۲۰۱۰) و قاهره (۲۰۱۱) حتی تصور گردهم‌آیی‌های چند میلیونی اعتراضی بدون استفاده از فیس‌بوک، توییتر و یوتیوب ناممکن بود.

شبکه‌های اجتماعی ابزارهای درخشان فعالیت مدنی‌اند، اما در عین حال شمشیر دولبه‌ای هستند که می‌توانند علیه فعالان مدنی عمل کنند.

دولت جمهوری اسلامی ایران از طرق مشابه روش‌های زیر، سایت‌هایی نظیر فیس‌بوک را علیه فعالان منتقد به کار می‌گیرد:

• Impersonation یا جا زدن خود به جای دیگری، ده‌ها و صدها شناسه مجعول با تصاویر افراد مشهور نظیر سیدمحمد خاتمی، رضا پهلوی، میرحسین موسوی، سمبل‌های اسلامی، هخامنشی، آذری، تیم‌های فوتبال، خوانندگان و یا بازیگران مشهور ایجاد می‌شود. در این شناسه‌ها با الفاظی زننده به رقبای سیاسی توهین می‌شود تا امکان هر نوع گفتگو و تعامل میان مخالفان از میان برود.

مثال: در اردیبهشت ماه سال ۱۳۹۰ صفحه‌ای جعلی با نام دکتر اردشیر امیرارجمند از چهره‌های سرشناس منتقد دولت ایران آغاز به عضوگیری نمود. این شناسه در فاصله کوتاهی با واکنش سریع امیرارجمند و اعلام گسترده در رسانه‌های منتقد دولت، جعلی اعلام شد. اما نگاهی به لیست افرادی که دعوت این شناسه را قبول کرده بودند، نشان می‌دهد حتی بسیاری از روزنامه‌نگاران و فعالان سرشناس نیز به سادگی با اعمال شیوه‌های ساده نفوذ اطلاعاتی در شبکه‌های اجتماعی، فریب خواهند خورد.

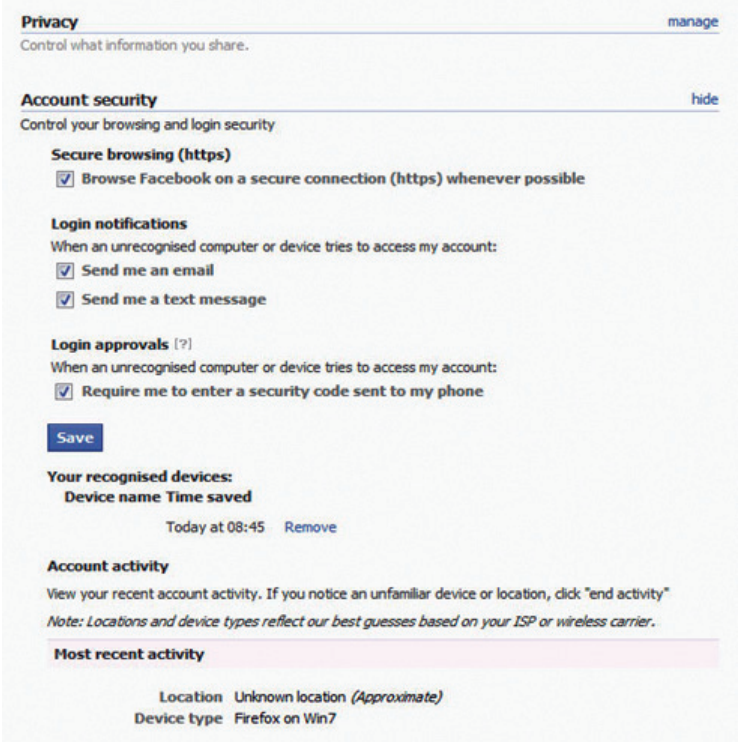
• در مواردی از یک شناسهٔ provocateur، توهین به مقدسات دینی، باورهای قومی، فرهنگی و سیاسی بخشی از شهروندان صورت می‌پذیرد، تا رضایت عمومی از سرکوب مخالفان حاصل آید.

• شناسه‌هایی با تصاویر جذاب و بعضا نیمه‌عریان دختران ایجاد می‌شود تا با شبکه گسترده‌ای از فعالان سیاسی تماس برقرار شده و اطلاعات آنلاین ایشان جمع‌آوری شود.
• شناسه‌ای جعلی به نام شما ایجاد شده و دوستان لیست شما مجددا دعوت می‌شوند.
• شناسه جعلی مثلا وارد گروه ۲۵ بهمن می‌شود و برخی از افراد آنجا را به لیست خود دعوت می‌کند. پس از آن به گروه ندای سبز آزادی می‌رود و تعدادی دعوت از آنجا می‌گیرد و به همین شکل با رفت و آمد میان گروه‌ها، شبکه خود را گسترده می‌کند.

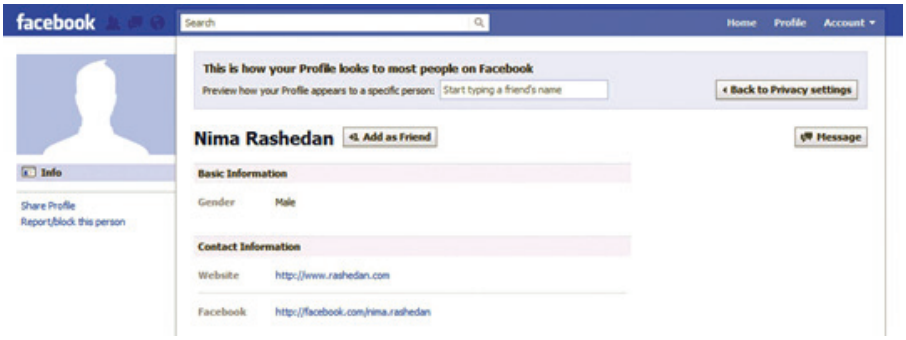
نکات ضروری برای فعالیت در شبکه‌های اجتماعی نظیر فیس‌بوک

فیس‌بوک امکانات متعددی را برای محافظت از امنیت اکانت شما، اضافه نموده است. استفاده از امکانات زیر قویا توصیه می‌شود:

۱. فیس‌بوک را برای استفاده امن https تنظیم کنید.
۲. تنها از یک کامپیوتر برای دسترسی به فیس‌بوک خود استفاده کنید؛ این کامپیوتر را در لیست دستگاه‌های مجاز خود ثبت کنید تا اگر فرد دیگری از کامپیوتر دیگری برای ورود به فیس‌بوک تلاش کرد، با ارسال SMS از این اقدام مطلع شوید.
۳. لیست افراد و کامپیوترهایی را که اخیرا به اکانت شما دسترسی داشته‌اند، دائما کنترل کنید.



۴. نمایش صورت کامل دوستان، اشتباه‌ترین عمل ممکن است. فرض کنید صورت اسامی دوستان یک فعال سیاسی صاحب‌نام به صورت عمومی نمایش داده شود؛ با این کار جان صدها و بلکه هزاران فعال سیاسی ساکن ایران به خطر خواهد افتاد. بلافاصله نمایش عمومی دوستان خود را متوقف کنید؛ لزومی به نمایش دوستان شما برای هیچ کس نیست. حتی بسیاری از دوستان شما نیز مایل به نمایش نام خود در مجموعه دوستان شما نیستند.



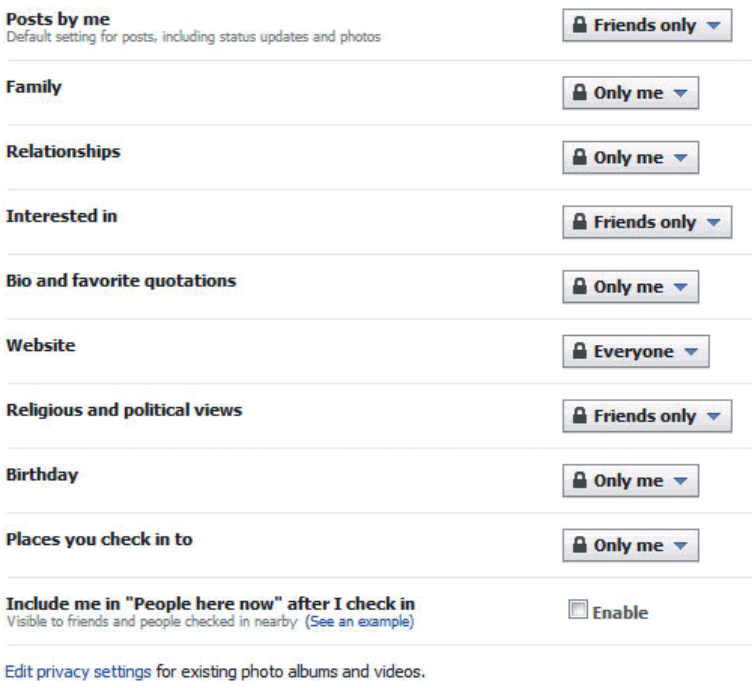
۵. نام خود را دائما در فیس‌بوک جستجو کنید. اگر کسی با نام و تصاویر شما مشغول فعالیت و گسترش شبکه در فیس‌بوک است، این حادثه را سریعا به فیس‌بوک گزارش کنید و از دوستان خود نیز بخواهید که گزارش این اقدام را برای فیس‌بوک ارسال کنند. این کار به سادگی و تنها با چند کلیک میسر است. این افراد با نام جعلی شما، با دوستان واقعی شما مرتبط شده و از آنان کسب اطلاعات می‌کنند.

۶. افراد ناشناس را اساسا به لیست خود اضافه نکنید. اگر روزنامه‌نگار و فعال سیاسی هستید و می‌خواهید که مخاطبان خود را در لیست داشته باشید، شناسه‌های دوم و سومی برای این کار ایجاد کنید. شناسه حاوی اطلاعات شخصی و خانوادگی شما به هیچ وجه نباید در معرض مشاهده افراد ناشناس قرار گیرد.

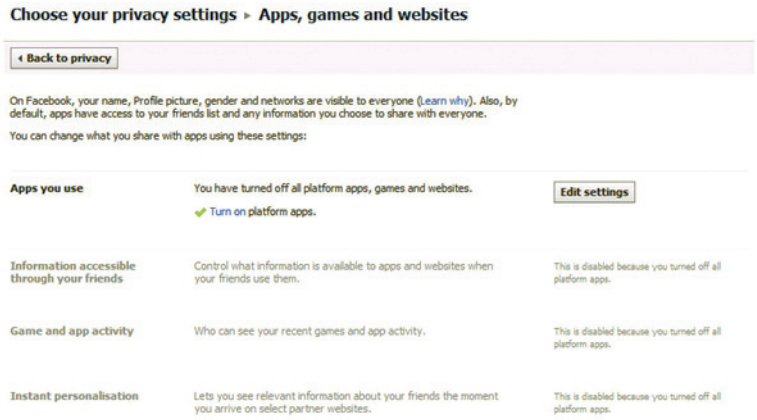
۷. از هویت واقعی دوستان خود قبل از اضافه کردن به لیست اطمینان حاصل کنید. پس از افزودن فردی که با تصویر دوست شما ظاهر شده است، او به بسیاری از اطلاعات شما دسترسی خواهد داشت. حذف او پس از اطلاع از جعلی بودن شناسه وی، کمکی در مورد اطلاعات از دست رفته شما نخواهد کرد.

۸. تاریخ تولد و محل سکونت خود را در پروفایل عمومی خود منتشر نکنید. بانک‌ها و مؤسسات

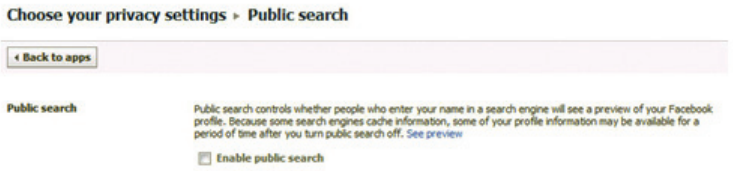
اینترنتی از همین دو داده برای ارسال مجدد پسورد فراموش شده شما و یا تغییر این پسورد و دسترسی به داده‌های حساس استفاده می‌کنند.



۹. حتی الامکان از برنامه‌های کاربردی Third Party Application در شبکه‌های اجتماعی استفاده نکنید. این برنامه‌ها می‌توانند به اطلاعات خصوصی شما دستیابی پیدا کنند. در قسمت تنظیمات امنیتی می‌توانید مانع از این امر شوید.



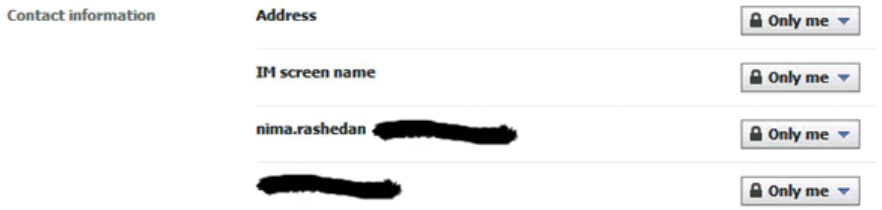
۱۰. اجازه ندهید نام شما در جستجوهای فیس‌بوک و موتورهای جستجو نظیر گوگل به نمایش درآید. در قسمت تنظیمات امنیتی می‌توانید از این کار جلوگیری کنید.



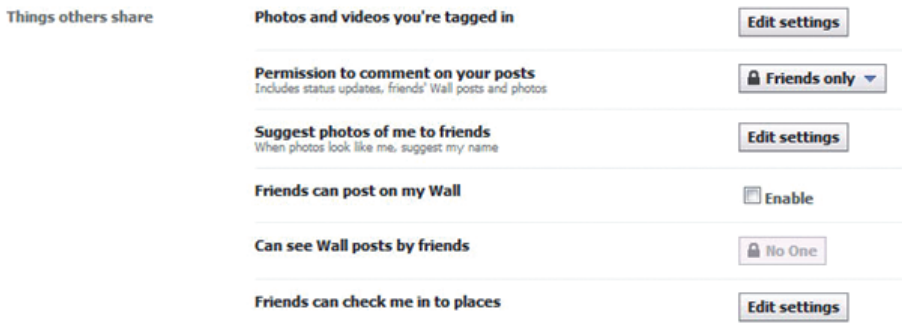
۱۱. می‌توانید صورت دوستان مختلفی تنظیم کنید؛ مثلا فعالان مدنی، روزنامه‌نگاران، دوستان نزدیک و غیره. می‌توانید سطح دسترسی این لیست‌ها را تغییر دهید؛ مثلا برخی از این گروه‌ها قادر به مشاهده آلبوم خاصی نباشند.

۱۲. قسمت Ralationship status خود را غیرفعال کنید.

۱۳. از نمایش عمومی شماره تلفن و آدرس ایمیل خود خودداری کنید.



۱۴. دسترسی کاربران به مشاهده پست‌های Wall و همچنین نوشتن پست بر Wall خود را محدود کنید.



۱۵. نمایش اطلاعات خود روی قسمت social ads را متوقف کنید.

۱۶. فهرست دوستان خود را با تغییر تنظیمات حریم خصوصی، از چشم دیگران پنهان نگه دارید تا بررسی و تحلیل حلقه ارتباطی شما به سادگی میسر نباشد. در غیر این صورت، حتی کسانی که در

فهرست دوستان شما نیستند، می‌توانند به لیست دوستان فیس‌بوکی شما دسترسی داشته باشند.

علاوه بر موارد فوق، استفاده از سرویس شبکه‌های اجتماعی همراه با تلفن‌های هوشمند و کامپیوترهای قابل حمل نیز نیازمند دقت مضاعف و رعایت مواردی است که قبلا درباره رسانه‌های قابل حمل گفته شد.

این اینفوگرافیک اطلاعات جالبی درباره تهدیدهای فیس‌بوکی برای کاربران دارد:

http://blog.trendmicro.com/the-geography-of-social-media-threats

اهمیت تنظیمات حریم خصوصی فیس‌بوک

محیطی که برای تغییر تنظیمات حریم خصوصی کاربران در فیس‌بوک طراحی شده، همواره دستخوش تغییر می‌شود و کاربران فعال و اکتیویست‌های سایبری باید با چک کردن مستمر اخبار و اطلاعات پیرامون آن و تست کردن امکانات جدیدی که اضافه می‌شوند، دانش خود در این زمینه را به‌روز کنند.

تسلط بر تنظیمات حریم خصوصی برای همه کاربران فیس‌بوک اهمیتی حیاتی دارد. اگر می‌خواهید جزئیات و راهنمایی‌های بیشتری در این باره بخوانید، این مطلب را از دست ندهید. «۱۰ نکته‌ای که باید درباره تنظیمات حریم خصوصی در فیس‌بوک بدانید»:

http://www.dw.de/dw/article/0,,6434375,00.html

توصیه‌هایی برای فعالان سایبری فعال در فیس‌بوک

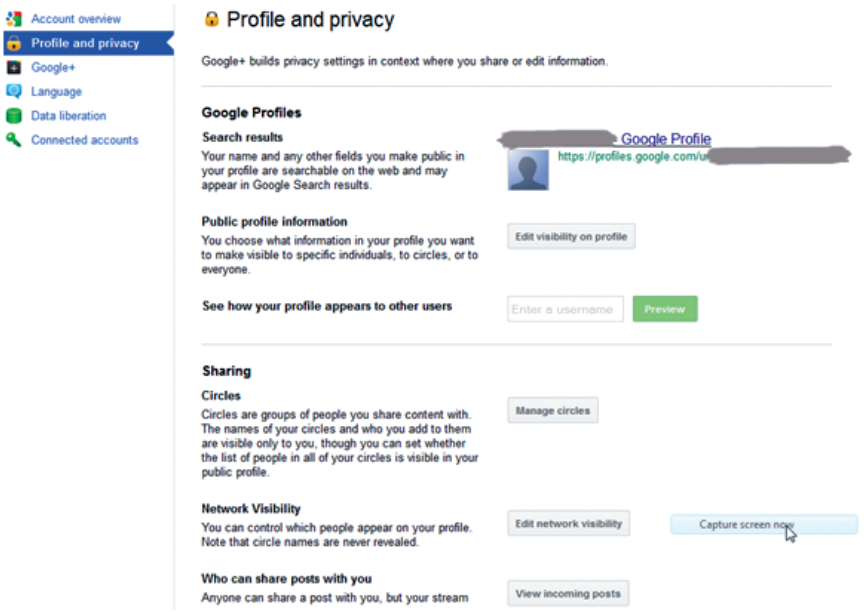
اگر از جمله کسانی هستید که با مدیریت صفحات گوناگون، از فیس‌بوک برای اکتیویسم آنلاین هم بهره می‌گیرید، باید دقت بیشتری به مساله امنیت و حریم خصوصی داشته باشید. در این مطلب، توصیه‌هایی برای افزایش امنیت اکتیویست‌ها در فیس‌بوک ارائه شده که خواندن آن توصیه می‌شود. «ایمن‌سازی حضور اکتیویست‌ها در فیس‌بوک»:

http://www.dw.de/dw/article/0,,14988781,00.html

امنیت گوگل پلاس (Google+)

شرکت گوگل سرویس شبکه اجتماعی خود، یعنی گوگل پلاس را از سال گذشته آغاز نمود، تجربه نشان می‌دهد در ماه‌های ابتدایی شروع به کار یک شبکه و یا سرویس، به دلیل عدم آشنایی کاربران، تبهکاران بسیاری به اینگونه شبکه‌ها هجوم می‌آورند، رعایت نکات ذیل به هنگام استفاده از گوگل پلاس ضروری است:

تنظیمات امنیتی گوگل پلاس به طور خلاصه بر پایه تنظیمات امنیتی اکانت شما بوده و در آدرس https://plus.google.com/settings/privacy قابل دسترسی و تغییر است.

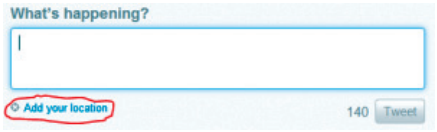


بر خلاف فیس‌بوک، در گوگل پلاس شما می‌توانید دوستان خود را در گروه‌ها یا حلقه‌های مختلفی سازماندهی کنید، بدون اینکه مشکل تداخل با اعضای حلقه‌های دیگر را داشته باشند. نکته قابل توجه دیگر گوگل پلاس، دسترسی کامل شما به داده‌هایتان است؛ شما می‌توانید عکس‌ها و سایر اسناد خود را یک جا دانلود کنید. آدرس داده‌های شما در گوگل پلاس:

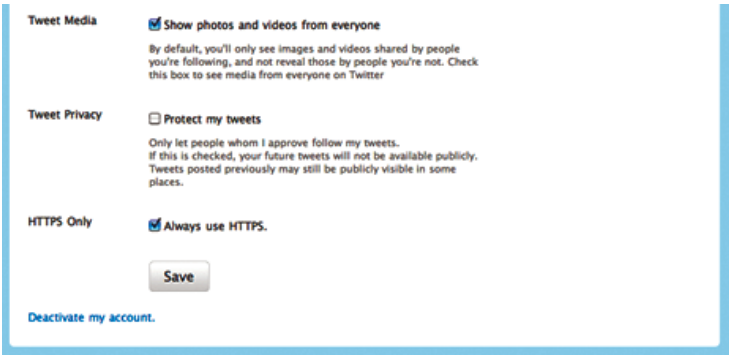
https://plus.google.com/settings/exportdata

امنیت در توییتر

توییتر، سرویس مایکروبلاگینگ و شبکه اجتماعی محبوبی که بیش از ۲۵۰ میلیون کاربر دارد، امکانات خارق‌العاده‌ای برای اطلاع‌رسانی، هماهنگی و سازماندهی نیروهای اجتماعی و سیاسی ارائه می‌کند. اما دولت‌های سرکوبگر همواره در کمین کاربران توییتر نشسته‌اند تا در شرایط اضطراری، با رهگیری و تعقیب و بازداشت آنها، از آسیب‌پذیری‌های امنیتی خود بکاهند. به همین خاطر لازم است که کاربران توییتر چند نکته مهم را به خاطر داشته باشند. اول اینکه اگر از کشوری مانند ایران توییت می‌کنید، حتما امکان مکان‌یابی را غیرفعال کنید، چون زمانی که این امکان فعال است، موقعیت جغرافیایی شما به همراه هر توییت ارسال می‌شود و این به شدت از ضریب امنیت شما می‌کاهد و تعقیب شما را برای نیروهای امنیتی وابسته به حکومت بسیار ساده‌تر خواهد کرد:



نکته بسیار مهم دیگر این است که باید با مراجعه به بخش تنظیمات، یک بار برای همیشه HTTPS توییتر را فعال کنید تا از این به بعد از هر سیستمی که به توییتر متصل می‌شود، از نسخه امن آن استفاده کنید. همان طور که می‌بینید، این کار به سادگی با چند کلیک میسر است:



نکته بسیار مهم دیگر اینکه اگر از اتصالات وایرلس ناشناس و بدون رمز استفاده می‌کنید و قصد دارید مثلا در یک تجمع اعتراضی از طریق موبایل خود توییت کنید، همواره به خاطر داشته باشید که با مرورگر موبایل خود وارد سایت توییتر شوید، نه از طریق اپلیکیشن؛ چرا که اپلیکیشن‌های موبایل و تبلت‌ها برای فیس‌بوک و توییتر معمولا رابط کاربری خاص خود را دارند و از نسخه HTTPS وارد سایت نمی‌شوند. به همین خاطر ممکن است اطلاعاتی که ارسال می‌کند توسط کسی که اتصال وایرلس خود را باز گذاشته است، کنترل شود. بنابراین از طریق مرورگر و با HTTPS وارد شوید تا اطلاعات کدگذاری شوند و امنیت شما افزایش یابد.

حذف همه توییت‌ها با چند کلیک

اگر تحت فشار قرار گرفتید یا احساس می‌کنید ممکن است به زودی با نیروهای امنیتی مواجه شوید و توییت‌های شما به هر دلیلی برای شما دردسر شود، می‌توانید با استفاده از ابزاری نظیر Tweetwipe به سرعت همه توییت‌هایی که روی اکانت خود ارسال کرده‌اید را پاک کنید. این ابزار از اینجا قابل دسترسی است: http://twitwipe.com/

مدیریت حضور در شبکه‌های اجتماعی

اگر می‌خواهید زندگی دیجیتال در شبکه‌های اجتماعی و حضور خود در این محیط‌ها را مدیریت کنید و انتشار پست‌ها در فیس‌بوک و توییتر را با نظم و هماهنگی بیشتری دنبال کنید، می‌توانید از برنامه‌های جانبی قدرتمندی نظیر هوت‌سویت (HootSuite) استفاده کنید. هوت‌سویت به خاطر رابط خاص کاربری، گاه امکان عبور از سد فیلترینگ را هم به کاربران کشورهایی نظیر ایران می‌دهد.

به‌سادگی می‌توانید از طریق آدرس http://hootsuite.com وارد این سرویس شوید و حتی اگر اکانتی ندارید، با اکانت جی‌میل خود وارد محیط کاربرپسند آن شوید. سپس اکانت‌های گوناگون توییتر

و فیس‌بوک خود را به آن معرفی می‌کنید و می‌توانید از امکانات کم‌نظیرش لذت ببرید و برای بهبود و ارتقای فعالیت‌های خود از آنها استفاده کنید.

اطلاعات کامل مرتبط با برنامه هوت‌سویت را می‌توانید از اینجا بخوانید:
http://www.dw.de/dw/article/0,,6395966,00.html

امنیت در فرندفید

فرندفید اگرچه هیچ امکان خاصی به کاربران ارائه نمی‌کند، اما همچنان در میان طیفی از کاربران ایرانی محبوبیت خود را حفظ کرده است. اما نکته اینجاست که این شبکه اجتماعی که حالا در تملک کمپانی فیس‌بوک است، به‌شدت ناامن و نامطمئن است و آسیب‌پذیری‌های امنیتی فاحشی دارد.

اگر بلاگر، روزنامه‌نگار یا فعال اجتماعی و سیاسی هستید، بهتر است از فرندفید استفاده نکنید و فعالیت‌های خود را در فیس‌بوک، توییتر یا گوگل پلاس پیگیری کنید. اما اگر همچنان به استفاده از این شبکه اجتماعی اصرار دارید، باید بدانید که یکی از ضعف‌های امنیتی موجود در آن، به کاربران این امکان را می‌دهد که به سادگی دایرکت مسج‌ها یا پیام‌های مستقیم شما را بخوانند. بنابراین هرگز از دایرکت مسج فرندفید برای ارسال اطلاعات حساس استفاده نکنید.

امنیت برای تلفن همراه و Smartphone

آموزش امنیت به کاربران تلفن‌های هوشمند و تبلت‌ها

تقریبا همه بررسی‌های انجام شده نشان می‌دهد کاربران امنیت تلفن‌های هوشمند و تبلت‌های خود را به اندازه کامپیوترهای شخصی جدی نمی‌گیرند. بسیاری از کاربران حتی نمی‌دانند ویروس‌های تلفن همراه وجود خارجی دارند. آنان لزومی هم به نصب آنتی‌ویروس، پسوردهای قوی و حتی فایروال احساس نمی‌کنند. اما حقیقت این است که دستگاه تلفن همراه شما قطعا از کامپیوترهای شخصی آسیب‌پذیرتر است. استفاده از تلفن‌های هوشمند و تبلت‌ها در دو سال اخیر رشدی انفجاری داشته و به همان میزان تهدیدات امنیتی موجود در آنها نیز افزایش یافته است.

توصیه‌های ایمنی زیر دانشجویان را در پاسخ دادن به تهدیدهای عمده تلفن‌های همراه و تبلت‌ها یاری می‌کند.

• سیستم عامل و تمام اپلیکیشن‌های خود را همیشه به روز نگاه دارید. این مهمترین توصیه امنیتی برای کاربران وسایل و تجهیزات موبایل است.

• تنها اپلیکیشن‌های شناخته شده و خوش‌نام را خریداری کنید. اپلیکیشن‌های گمنام خطرناک‌اند.

• اپلیکیشن‌ها را از فروشگاه‌های رسمی و قانونی سیستم عامل تلفن همراه و یا تبلت خود خریداری کنید؛ مثل آی‌تونز یا آندروئید مارکت.

• قبل از نصب اپلیکیشن نظر کاربران این اپلیکیشن یا به اصطلاح فیدبک یا review آنان را مطالعه کنید.

• روی کامپیوتر تبلت و تلفن هوشمند خود فایروال نصب کنید.

• از پسوردهای قوی استفاده کنید.

• اگر با اطلاعات حساس سر و کار دارید از موبایل‌های کرک شده یا JailBreak استفاده نکنید.

• اگر با اطلاعات حساس سر و کار دارید از فروشگاه‌های آلترناتیو مثل Cydia دانلود نکنید.

• بلافاصله پس از استفاده از بلوتوث آن را خاموش و از مود بلوتوث خارج کنید.

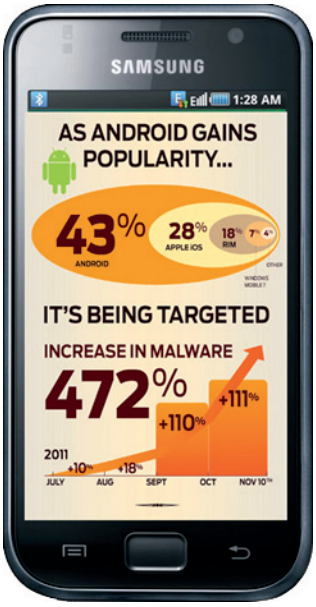
• یک برنامه مطمئن امنیت موبایل نصب کنید.

• به شبکه‌های WiFi عمومی و رایگان متصل نشوید.

• حالت WiFi Adhoc را حتی الامکان به کار نبرید و در صورت ضرورت بلافاصله خاموش کنید.

اگر می‌خواهید درباره ملاحظات امنیتی ضروری برای کاربران موبایل و تبلت‌ها بیشتر بخوانید و بدانید، این مطلب را از دست ندهید. «۱۰ نکته‌ای که کاربران موبایل شبکه‌های اجتماعی باید بدانند»: http://www.dw.de/dw/article/0,,15394437,00.html

موبایل‌ها و تبلت‌های آندروئید تهدید می‌شوند



همان‌گونه که در نمودار روبرو مشاهده می‌کنید تلفن‌های هوشمند آندروئید (سیستم‌عامل موبایل تولید کمپانی گوگل) که در میان کاربران محبوبیت بسیاری کسب کرده‌اند، در روندی بی‌سابقه تهدید می‌شوند. هزاران بدافزار مخصوص آندروئید تولید و از طریق اپلیکیشن‌های آلوده در بازارهای آندروئید پخش می‌شود. اگر چه گردانندگان این بازارها سعی می‌کنند تا اپلیکیشن‌های آلوده را بلافاصله پاک کنند، اما به هر حال به دلیل گستره عظیم استفاده از آندروئید پاکیزه‌سازی کامل بازاری که اساسا توسط کاربران اداره می‌شود، کار چندان ساده‌ای نیست.

تهدیدهای عمده علیه تلفن‌های آندروئید:

- ۵۵ درصد جاسوس‌افزارها
- ۴۴ درصد تروجان‌هایی ارسالی با اس‌ام‌اس

برای تلفن آندروئید خود نرم‌افزار امنیتی نصب کنید.

برنامه‌های رایگان آنتی‌ویروس برای موبایل آندروئید:

- Norton™ Mobile Security
- Lookout Antivirus
- DroidSecurity Anti virus
- AppScan

امنیت و تلفن‌های همراه

امروزه تصور زندگی و فعالیت روزمره بدون بهره‌گیری از خدمات تلفن‌های همراه ناممکن است. در کشوری مانند ایران امنیت استفاده از تلفن‌های همراه از سوی دستگاه‌های امنیتی دولتی و همچنین تبهکاران معمولی تهدید می‌شود.

تلفن‌های همراه در سال‌های اخیر به یکی از مهمترین ابزارهای کوشندگان دموکراسی در سراسر جهان تبدیل شده‌اند و هر روز بیش از پیش انتشار تصاویر سرکوب و خشونت علیه شهروندان به محکومیت جهانی دولت‌های سرکوبگر می‌انجامد.

نکته مثبت و در عین حال نگران‌کننده درباره تلفن‌های همراه، افزایش روزانه و چشمگیر پیچیدگی‌های تکنیکی این دستگاه‌هاست. تلفن‌هایی که تا چند سال پیش با استفاده از شبکه آنالوگ تنها قادر به مکالمه صوتی بودند، امروز علاوه بر سرویس‌های متنی (SMS) و یا مولتی‌مدیا (MMS)، صدها قابلیت جدید را عرضه می‌کنند.

تلفن‌های همراه جدید، قابلیت مکالمه در نرم افزارهای چت صوتی نظیر Skype، استفاده از انواع مسنجرها، استفاده از شبکه‌های اجتماعی مثل Facebook و تقریبا همه توانایی‌های کامپیوترهای شخصی را ارائه می‌دهند.

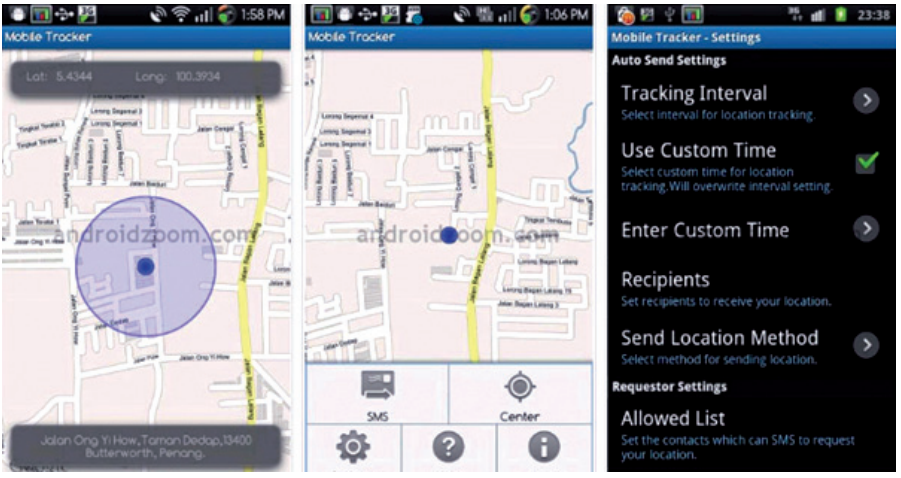
نرم افزار IM+، ارائه دهنده سرویس‌های مسنجر Twitter، Skype، Facebook، Google Talk، MySpace، AIM، ICQ، Yahoo!، MSN، Jabber با قابلیت نصب در تلفن‌های Android، Iphone، Symbian، Windows mobile، Blackberry است.

نرم افزار کاربردی Fring نیز نظیر IM+ قابلیت چت و چت صوتی را برای تلفن‌هایی نظیر Iphone، آندروئید و نوکیا Ovi ارائه می‌کند.

در اینفوگرافیک «آنچه باید درباره بدافزارهای موبایل بدانید» اطلاعات مفید و جالب بسیاری پیرامون این موضوع ارائه شده است:

http://mashable.com/2011/08/12/mobile-malware/

در تلفنهای همراه، حتی بیش از کامپیوترهای شخصی می‌توان از موقعیت دقیق فرد حامل تلفن به فاصله چند متری و همچنین افراد پیرامون وی اطلاع حاصل کرد.



فرض کنید هشت نفر از فعالان سیاسی شناخته شده در ایران از منزل خود خارج می‌شوند تا فعال شماره نه را که به صورت مخفی زندگی می‌کند، ملاقات کنند. دستگاه‌های دولتی در ایران قادر به رصد

کردن جغرافیایی این هشت شماره تلفن همراه هستند. فرض کنید در نقطه‌ای خلوت این هشت شماره تلفن با هم ملاقات می‌کنند. در استاندارد تلفن‌های سلولار، دستگاه‌های دولتی می‌توانند همه شماره‌هایی را که به لحاظ جغرافیایی در سلول مخابراتی نزدیک این هشت نفر هستند را شناسایی کنند و این به معنای کشف نفر نهم است. ساده‌ترین راه غلبه بر این مشکل همراه نبردن و یا خارج کردن باتری موبایل قبل از ترک منزل است. چاره دیگر، ملاقات در محلی نظیر ایستگاه‌های راه‌آهن و یا میدان‌های شلوغ است که دستگاه دولتی، هشت موبایل مورد نظر را میان هزاران موبایل ناشناس در تردد در اطراف ایشان رصد خواهد کرد.

برای درک بهتر رشد بی‌سابقه تهدیدات دیجیتال و بدافزارهای مختص موبایل‌ها و تبلت‌ها، این اینفوگرافیک را مشاهده کنید که در آن راهکارهایی نیز برای مقابله با این تهدیدات پیشنهاد شده است:

http://www.theatlantic.com/technology/archive/2011/09/infographic-protect-yourself-from-the-threat-of-mobile-malware/243998/

سرقت؛ بزرگ‌ترین تهدید تلفن‌های همراه

اساسی‌ترین آسیب امنیتی دستگاه موبایل شما سرقت است. سرقت موبایل حتی برای تازه‌کارترین سارقین، عمل بسیار ساده‌ای به شمار می‌آید. همیشه برای سرقت موبایل خود آمادگی کامل داشته باشید.

شماره افراد حساس را با نام و مشخصات کامل ذخیره نکنید. هیچ فیلم، تصویر و یا صوت حساسی را در حافظه تلفن خود ذخیره ننمایید، اگر ذخیره چنین کلیپی ضروری بود، بهتر است بلافاصله آن را در آرشیو آنلاین داده‌های حساس و کدگذاری شده خود ذخیره نموده و از تلفن پاک کنید.

به خاطر داشته باشید که صرف پاک کردن پیام‌های متنی، تصویری، صدا و دیگر اطلاعات به امحای دائمی آنها نخواهد انجامید. حتی برنامه‌هایی رایگان وجود دارند که می‌توانند پیام‌های متنی، تصاویر و سایر اطلاعات پاک شده در حافظه و یا حافظه کارتی موبایل‌ها را احیاء کند. در عین حال برنامه‌هایی نیز وجود دارند که می‌توانند امکان بازیافت این اطلاعات را از بین ببرند. برنامه پیشنهادی ما برای این کار نرم‌افزارهای عمومی wipe و به طور مشخص برنامه CCleaner است. با برنامه CCleaner و انتخاب گزینه دوباره‌نویسی تصادفی روی اطلاعات پاک شده، می‌توانید بازیابی مجدد آنان را ناممکن کنید.

در بسیاری از موارد، از موبایل به سرقت رفته شما می‌توان برای ورود به ایمیل، فیس‌بوک، مسنجرها و پیام‌گیر تلفنی Message Box شما استفاده کرد. بلافاصله پس از سرقت موبایل کد عبور همه موارد فوق را عوض کنید. از خاطر نبرید که در بسیاری از این سایت‌ها امکان تغییر مجدد کد با ارسال اس‌ام‌اس به موبایل سرقت شده وجود دارد، بنابراین به هنگام تغییر پسورد، شماره تلفن ذخیره شده خود را نیز تغییر دهید.

توصیه‌های کاربردی

۱. هرگز SIM PIN و Phone Security Code تلفن همراه خود را غیرفعال نکنید.

برخی از تلفن‌ها این قابلیت را دارند که پس از مفقود شدن و یا سرقت می‌توان آنها را با یک

اس‌ام‌اس قفل و از دسترس سارق خارج کرد. این قابلیت به طور مثال برای گوشی نوکیا N97 به شکل زیر است:

اکثر ارائه دهندگان سرویس موبایل، قادرند گوشی شما را در صورت سرقت، قفل و بلوکه نمایند. برای درخواست این کار می‌بایستی شماره گوشی و شماره سیم کارت خود را جایی یادداشت کرده باشید. اگر شماره گوشی یا IMEI خود را نمی‌دانید، *#06# را وارد نمایید تا روی صفحه موبایل شما به نمایش درآید.

در سال‌های اخیر نرم‌افزارهای بسیار کارآمدی ارائه شده است که به شما امکان می‌دهند تلفن به سرقت رفته یا گم شده خود را تا حد ممکن ردیابی و کنترل کنید، نمونه‌هایی از این نرم افزارها Theft Aware و GadgetTrak و Find my iPhone & iPad برای سیستم‌عامل iOS کمپانی اپل هستند.

۲. اطلاعات تلفن همراه خود را دائما در نسخه پشتیبان (Backup) ذخیره و سپس حافظه تلفن را wipe نمایید. wipe کردن در اصطلاح به انجام پروسه‌ای می‌گویند که بازیابی اطلاعات پاک شده از حافظه تلفن شما را ناممکن می‌کند. شما می‌توانید از نرم‌افزارهای رایگان که با روش‌هایی نظیر Zeros، Gutmann، US DoD 5220.22-M (ECE)، US DoD 5220.22-M (E)، Pseudorandom data و Royal Canadian Mounted Police DSX اطلاعات پاک شده حافظه‌های موبایل را برای همیشه غیرقابل بازیابی می‌نمایند، استفاده کنید. مثلا نرم‌افزار رایگان و کارآمد Wipe Free Space در آدرس http://wipefreespace.sourceforge.net/ در دسترس است.

نکات کلیدی در امنیت تلفن‌های همراه

• تلفن همراه و اصلی‌ترین استاندارد مورد استفاده در آن یعنی GSM حفره‌های ایمنی متعددی دارد. از تلفن همراه برای گفتگوهای حساس استفاده نکنید. استفاده از نرم‌افزارهای انتقال داده مثلا VOIP روی تلفن همراه و استفاده از استانداردهای پیچیده‌تر انتقال داده نظیر GPRS به امنیت بیشتر تلفن شما

کمک می‌کنند. همچنین با نصب برنامه کدگذاری مکالمات تلفن همراه می‌توانید شنود آن توسط دستگاههای دولتی را مشکل‌تر کنید. این تلفن‌های مجهز به نرم‌افزارهای کدگذاری دوسویهٔ داده‌های صوتی برای تلفن همراه، ENCRYPTED CELL PHONE نامیده می‌شوند.

• یکی از مشکلات امنیتی تلفن همراه امکان بسیار ساده تعقیب مکان جغرافیایی شما است اگر نمی‌خواهید مکان شما توسط دستگاههای دولتی کشف شود، باتری تلفن همراه خود را پس از خاموش کردن آن، خارج سازید.

توصیه‌های کاربردی

۱. استفاده از بلوتوث برای انتقال داده از موبایل به کامپیوتر و دستگاههای دیگر جانبی، سودمند اما مخاطره‌آمیز است. بلوتوث اساسا تکنولوژی امنی به حساب نمی‌آید. بسیاری از کاربران فراموش می‌کنند و یا اساسا نمی‌دانند پس از پایان ارتباط بلوتوث می‌بایستی وضعیت بلوتوث موبایل خود را خاموش کنند.

۲. در کافی‌نت‌ها، فرودگاه‌ها و اماکن عمومی به سیگنال‌های وایرلس مشکوک متصل نشوید. برخی از تبهکاران، Accsess point واسطه‌ای را با هدف تغییر DNSهای شما و ایجاد نوعی تونل برای ارتباط شما و اینترنت ایجاد می‌کنند. تمام اطلاعات تلفن هوشمند و یا دستگاه کامپیوتر شما برای واسطه فوق قابل رویت است.

۳. نه تنها تلفن‌های همراه، حتی تلفن‌های بی‌سیم خانگی با استاندارد DECT نیز به سادگی قابل شنود هستند. وقتی جلسه یا مکالمه محرمانه‌ای در کنار این دستگاه‌ها دارید، باتری آنها را خارج سازید.

۴. تلفن‌های هوشمند و همراه نیز چون کامپیوتر در معرض خطر انتقال ویروس از طریق میکرودیسک و یا وصل و سنکرونایز به کامپیوتر آلوده هستند. قبل از نصب میکرودیسک از پاکیزگی آن اطمینان حاصل کنید. میکرودیسک حاوی اطلاعات ضروری را همراه خود حمل نکنید. آن را از تلفن همراه خارج نموده و Backup ایجاد کنید.

ویروس‌های تلفن همراه

ویروس‌ها، برنامه‌های جاسوس و هرزنامه‌ها، همه امنیت تلفن‌های همراه را تهدید می‌کنند. تروجان‌های بسیاری برای تلفن‌های همراه ارسال شده است. برخی از این نرم‌افزارهای مخرب نظیر Fontal.a توسط یک MMS برای شما ارسال می‌شوند، بعد از باز کردن این MMS دستگاه تلفن شما ری‌بوت شده و امکان دسترسی نفوذکنندگان به داخل تلفن شما و دانلود و یا آپلود داده‌های تلفن را فراهم خواهد آورد. اغلب این ویروس‌ها، از طریق بلوتوث، MMS و یا اتصال به کامپیوتر و یا دانلود نرم‌افزار آلوده تکثیر می‌شوند.

Cabir.a	worm
velasco	worm, parasitic virus
Commwarrior a,b,c	worm
mabir.a	parasitic virus
Duts.a	parasitic virus
Brador.a	Trojan backdoor
Mosquito.a	Trojan
Skulls.a	Trojan
CabirDropper.a	Trojan + Worms
MGDropper.a	Trojan + Worms
Dampig	Trojan
Locknut.b	Trojan
rever.a	Trojan
Fontal.a	Trojan
Hobbes.a	Trojan
Nameoomboot.a	Trojan with worm
Onehop.a	Trojan with other trojan
Blankfont.a	Trojan
Fontal.c	Trojan
Nameoomboot.c	Trojan with worm
Nameoomboot.d	Trojan with worm
AppDisabler.a	Trojan
Cardtrap.d	Trojan
Caribe–	Worm
Trojan_Mos	Trojan

• در تلفن‌های همراه و هوشمند با نفوذ به داخل دستگاه شما، امکان دانلود لیست شماره‌ها، اس‌ام‌اس‌های دریافتی و ارسالی، فایل‌ها و حتی نصب نرم‌افزار شنود مکالمات وجود دارد.

نمونه‌هایی مشخص از آسیب‌پذیری‌های تلفن‌های هوشمند اپل

• آیفون‌ها و دیگر دستگاه‌های اپل که از سیستم‌عامل‌های قدیمی‌تر از ۳، ۴ و ۵ استفاده می‌کنند و اپل به آنان اجازه آپدیت شدن به سیستم‌های جدیدتر را نمی‌دهد، در معرض تهدید مشخص SSL MITM قرار دارند. متاسفانه در حال حاضر این خطر میلیون‌ها کاربر اپل را تهدید می‌کند، بدون آنکه چارهٔ خاصی برای ایشان اندیشیده شده باشد.

• حتی هفته‌ها پس از اعلام عمومی جعل گواهینامه‌ها توسط دولت ایران، مرورگر سافاری روی آیفون و آی‌پد، گواهینامه‌های جعلی Diginotar را به رسمیت می‌شناخت.

ضمیمه ۱
برنامه‌های رایگان برای امنیت داده‌ها

همه ما با فایل‌ها، ایمیل‌ها، تصاویر، ویدئوها و سایر داده‌هایی سر و کار داریم که به دلایل مختلف برای ما خصوصی تلقی می‌شوند. کنشگران مدنی و روزنامه‌نگاران ایرانی ممکن است به داده‌هایی دسترسی داشته باشند که توزیع عمومی آن موجب ایجاد دردسر و به خطر افتادن امنیت شهروندان دیگری شود.

تصور کنید، فایل متن یا تصویر حساسی روی لپ‌تاپ شما ذخیره شده است. سرقت این فایل در یکی از چهار شکل زیر امکان‌پذیر است:

۱. لپ‌تاپ شما سرقت شود.

۲. فردی با سوءاستفاده از غیبت شما، وارد لپ‌تاپ شود و فایل را روی یک حافظه فلش ذخیره کند.

۳. کامپیوتر شما مورد حمله هکری قرارگرفته، فردی با دسترسی غیرمجاز از راه دور، مثلا از طریق اینترنت داده‌های شما را به کامپیوتر خود منتقل کند.

۴. خود شما به صورت اشتباه و سهوا، فایل حساس را در اختیار عموم قرار دهید.

بسیاری از کاربران تصور می‌کنند که مورد سوم، یعنی «حملات هکری» خطرناک‌ترین تهدید امنیت داده‌هاست. تصوری که الزاما درست نیست. هکرها خطرناکند اما آگاهی عمومی نسبتا مناسبی میان کاربران معمولی کامپیوتر علیه حملات هکری وجود دارد. بسیاری از کاربران آنتی‌ویروس و فایروال‌های کارآمدی روی کامپیوتر خود نصب کرده‌اند. مرورگرها و سیستم‌های عامل روز به روز امن‌تر می‌شوند و امکان به روزرسانی آنلاین کامپیوتر شما را در برابر حملات نوظهور هکری محافظت می‌کنند.

اما شما چند کاربر کامپیوترهای شخصی را می‌شناسید که داده‌های خود را در برابر خطر «سرقت لپ‌تاپ»، محافظت و ایمن‌سازی کرده باشند؟ کدامیک از دوستان شما، داده‌های خود را قبل از انتقال به فلش دیسک، هارد دیسک‌های اکسترنال و سایر ابزارهای ذخیره و انتقال اطلاعات کدگذاری می‌کنند؟

فلش دیسک‌ها بسیار کوچک هستند و به سادگی ممکن است گم شوند. برای خواندن و انتشار فلش دیسک محافظت نشده‌ای که از جیب یا جاکلیدی شما به زمین می‌افتد، فقط لازم است آن را به یک کامپیوتر شخصی متصل کرد.

برای مقابله با همه خطرات بالا، ترفندهای کمابیش موثری وجود دارند:

• داده‌های حساس خود را به نوعی کدگذاری و ذخیره نمائید که حتی در صورت سرقت احتمالی لپ‌تاپ، برای سارقین قابل استفاده نباشند.

• شما می‌توانید با رمزگذاری مناسب و ذخیره‌سازی آنلاین داده‌های حساس این امکان را که فردی در غیاب شما به اطلاعات دسترسی پیدا کند به حداقل برسانید.

• با شیوه‌های فریب «مهندسی اجتماعی» آشنا شوید تا خود به دست خود زمینه نفوذ تبهکاران را فراهم نیاورید.

• کامپیوتر و داده‌های خود را در برابر نفوذ احتمالی هکرها به آخرین تکنولوژی موجود مجهز نمائید.

• حیطه‌بندی اطلاعات را بشناسید و داده‌های خود را مثلا در شبکه‌های اجتماعی با افراد ناشناس به اشتراک نگذارید.

برای مقابله با همه خطرات بالا، ترفندهای کمابیش موثری وجود دارند، در این بخش ترفندهای موثری را برای محافظت از داده‌های شما معرفی می‌کنیم.

داده‌های شما در وسایل زیر ذخیره شده‌اند:

• ذخیره آنلاین مثلا ایمیل‌های شما روی جی‌میل یا اطلاعات شما روی فیس‌بوک
• هارد دیسک داخلی کامپیوتر
• هارد دیسک اکسترنال
• فلش درایو
• CD یا DVD
• کارت‌های حافظه داخل تلفن همراه نظیر SIM CARD یا MicroSD
• کارت‌های حافظه وسایل دیگر نظیر کارت‌های داخل دوربین دیجیتال یا ضبط صوت و غیره.

جلوگیری از انتقال بدافزار توسط حافظه‌های اکسترنال

Panda USB Vaccine

برای جلوگیری از انتقال و ورود بدافزار به صورت اتوماتیک به هنگام اتصال حافظه‌های خارجی نظیر فلش درایو، هارد اکسترنال، حافظه دوربین و یا MicroSD موبایل، برنامه ساده و بسیار پرقدرت

زیر را نصب کنید:

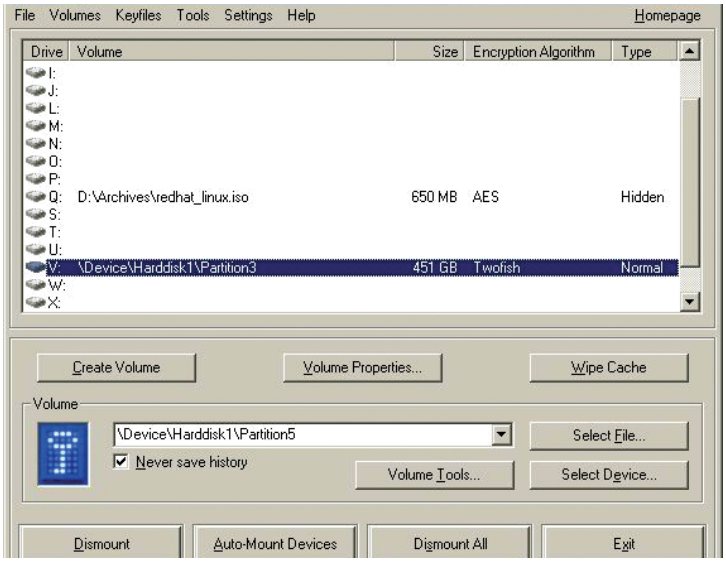
برنامه Panda USB Vaccine کامپیوتر شما و همچنین هر فلش درایو، هارد اکسترنال یا حافظه قابل خواندن و نوشتنی که به کامپیوتر شما متصل شود را در برابر انتقال اتوماتیک بدافزار با استفاده از قابلیت Autorun واکسینه می‌کند.

برای اطلاع بیشتر از نصب و تنظیمات این برنامه به ویدئوهای آموزشی توانا مراجعه کنید.

کدگذاری داده‌های حساس

TrueCrypt

نرم افزار رایگان کدگذاری TrueCrypt به صورت رایگان شما را قادر به کدگذاری حافظه‌های



فلش، هارد دیسک و هر نوع حافظه ذخیره‌سازی می‌کند. استفاده از TrueCrypt داده‌های شما را در برابر تلاش برای ورود با تایپ مجدد پسورد یا نرم افزارهای پسوردشکن نیز ایمن می‌کند.

TrueCrypt از مهم‌ترین برنامه‌های رمزگذاری و پنهان‌سازی فایل‌ها است و امکانات بسیار جالب و کم‌نظیری به کاربران ارائه می‌دهد.

ذخیره‌سازی و پردازش داده‌ها روی ابرِ آنلاین

Cloud Computing

در تکنولوژی پردازش ابری، روز به روز وابستگی شما به دستگاه‌های ذخیره‌سازی اطلاعات نظیر هارد دیسک کاهش یافته، اطلاعات و حتی برنامه‌های کاربردی شما روی سرورهای ابر، ذخیره و یا اجراء می‌شوند.

شما احتمالا با پردازش و ذخیره‌سازی ابری، آشنایی دارید. سال‌ها پیش از ظهور جی‌میل، سرویس ایمیل گوگل، برنامه‌هایی نظیر Outlook ایمیل‌های شما را از سرور ایمیل شما دانلود و روی هارد دیسک ذخیره می‌کردند، امروز جی‌میل، پست الکترونیکی شما را ذخیره می‌کند و نیاز چندانی به ذخیره ایمیل‌ها روی هارد دیسک نیست. سرویس‌های آنلاین دیگر گوگل نظیر Google Docs نیز تلاش دارند جایگزین برنامه‌های آفلاین مشابه نظیر Microsoft Office شوند. به همین دلیل شرکت مایکروسافت نیز با ورود به این عرصه، برنامه‌هایی نظیر Office 365 را ارائه نموده است.

مشاهده این ویدئو می‌تواند به افزایش امنیت Google Docs شما کمک شایانی کند:

http://www.youtube.com/watch?v=qo-ZrbrAhDI

استفاده از «ابر» را به دو شرط ذیل توصیه می‌کنیم:

الف: به اینترنت پرسرعت دسترسی دارید.

ب: شیوه مناسبی برای حفظ رمزهای کامپیوتر خود نزد دوستان و بستگان خود در خارج از ایران یافته‌اید.

شما در صورت دسترسی به اینترنت پرسرعت می‌توانید، داده‌های حساس، ایمیل‌ها، تصاویر، موزیک و ویدئوهای خود را روی «ابر» ذخیره کرده و با دوستان خود به اشتراک بگذارید. یکی از مشهورترین این

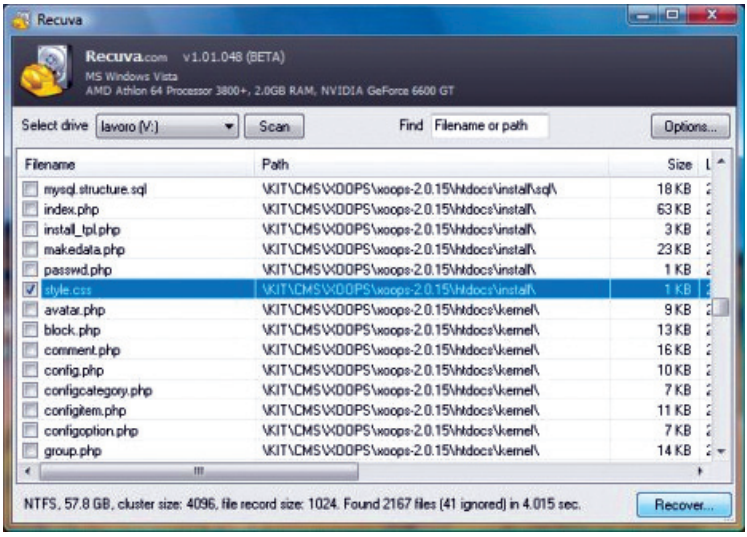
سرویس‌ها Dropbox است. ترکیبی از Dropbox و TrueCrypt می‌تواند برای شما فضای ذخیره‌سازی آنلاین، به علاوه امکانات کدگذاری را فراهم آورد. توجه داشته باشید که سرویس‌های مشابهی امکان ذخیره اطلاعات کدگذاری شده را ارائه می‌دهند، فهرست سرویس‌های Backup و ذخیره‌سازی آنلاین را از این آدرس می‌توانید مشاهده نمایید.

http://en.wikipedia.org/wiki/List_of_online_backup_services

بازیافت داده‌های پاک شده

Recuva[1]

نرم افزار recuva ابزار بسیار جالبی برای بازیافت داده‌هایی است که به اشتباه پاک شده‌اند؛ مثلا عکس‌هایی که قبل از انتقال به کامپیوتر، از دوربین دیجیتال خود پاک کرده‌اید. یا فایل‌های موزیک و... که سهوا پاک شده‌اند.



درباره بازیافت داده‌های پاک شده، نکته جالب توجه اینکه هر اندازه فاصله زمانی میان پاک کردن داده‌ها و تلاش برای بازیافت آن کمتر باشد، احتمال موفقیت بازیافت بیشتر است. هر اندازه داده‌های کمتری پس از پاک کردن داده‌ها روی حافظه نوشته شده باشد نیز این احتمال یعنی موفقیت در بازیافت بیشتر است.

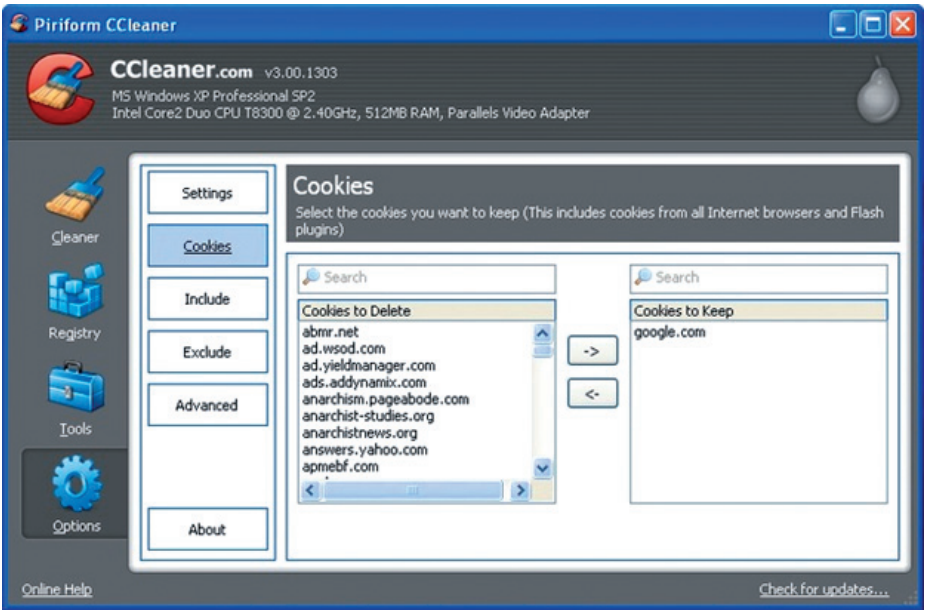
مثلا اگر یک کول دیسک USB حاوی عکس‌های شما بوده است و پس از پاک کردن عکس‌ها آن را با موزیک پر کرده باشید. شانس بازیافت عکس‌های اولیه صفر است، چرا که روی آنها داده‌های دیگری نوشته شده است.

1. www.piriform.com/recuva

غیرقابل بازیافت کردن داده‌های پاک شده

CCleaner[1]

CCleaner را برای غیرقابل بازیافت کردن داده‌های خطرناک و حساس روی هارد دیسک یا وسایل دیگر ذخیره‌سازی به کار برید. این عمل، یعنی پاک کردن دائمی داده‌ها را اصطلاحا wipe می‌گویند. مثلا دوربین دیجیتال خود را فروخته‌اید یا قصد هدیه دادن آن را دارید و نمی‌خواهید کسی قادر به بازیافت داده‌های پاک شده روی کارت حافظه باشد. یک راه بیرون آوردن و شکستن کارت حافظه است، راه دوم استفاده از نرم افزار CCleaner است.



این نرم افزار قادر است، فایل‌های کمکی مرورگرهای شما را پاک کند و فایل‌های پاک شده شما را نیز برای همیشه غیرقابل بازیافت نماید. این نرم‌افزار همچنین توان پاک کردن داده‌های اضافی در رجیستری و همچنین استارت‌آپ کامپیوترهای ویندوز را نیز دارد.

استفاده از CCleaner توصیه می‌شود، چرا که علاوه بر ارتقاء امنیت داده‌های شما با پاک کردن داده‌های غیرضروری و پیرایش رجیستری کامپیوتر شما، سرعت عمومی کامپیوتر و حتی سرعت دانلود صفحات وب را نیز تا حدی بالا خواهد برد.

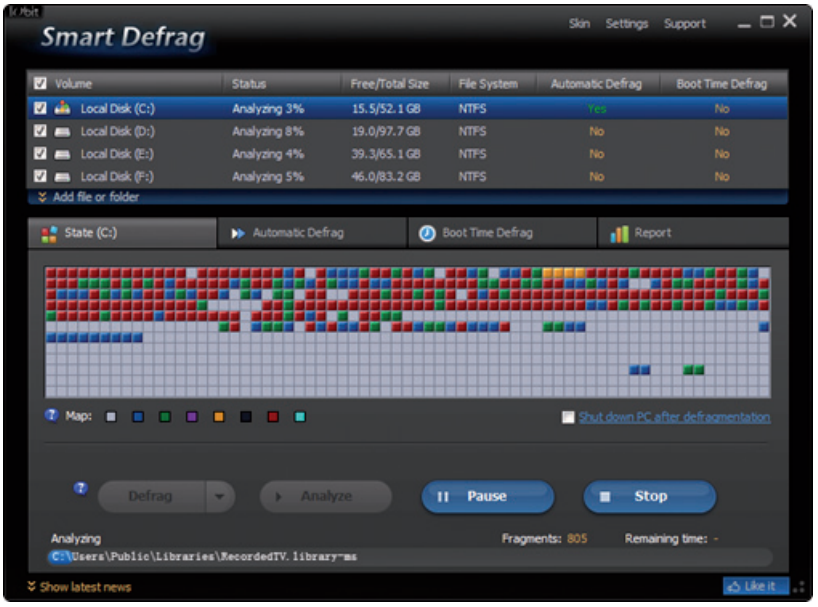
1. www.piriform.com/ccleaner

افزایش سرعت هارد دیسک با Defrag

Smart Defrag[1]

با گذشت زمان و استفاده از کامپیوتر، داده‌ها روی هارد دیسک‌های شما به صورت پراکنده توزیع می‌شوند، این پراکندگی داده‌ها، می‌تواند موجب فعالیت مداوم هارد دیسک و کاهش سرعت کامپیوتر شود. سیستم عامل ویندوز خود برنامه‌ای به نام Defrag را برای کاربران ویندوز طراحی نموده است که از قسمت system tools ویندوز قابل استفاده است. ما برنامه Smart Defrag را به دلیل کارایی فراتر و سهولت استفاده توصیه می‌کنیم.

این برنامه رایگان داده‌های پراکنده روی هارد دیسک شما را منظم کرده و به صورت یکپارچه و دسته‌بندی شده، مجددا بازنویسی می‌کند. یک روش خوب برای افزایش سرعت هارد دیسک، اجرای اتوماتیک این برنامه پس از هر بار restart کردن کامپیوتر است.



1. www.iobit.com/iobitsmartdefrag.html

ضمیمه ۲
برنامه‌های قابل حمل برای امنیت بیشتر

نرم‌افزارهای کدباز و قابل حمل (Portable)

نرم‌افزارهای کدباز به گروهی از نرم‌افزارها گفته می‌شود که تهیه‌کننده آن، کد برنامه‌نویسی را به صورت رایگان در اختیار کاربران قرار می‌دهد. انتشار نرم‌افزارهای کدباز در سال‌های گذشته امکان انتخابی جدی برای کاربرانی قرار داده است که به دلایل متفاوت قصد صرفه‌جویی در هزینه خرید نرم افزارها را دارند. در این ضمیمه تعدادی از نرم‌افزار کدباز را به عنوان مثال معرفی کرده‌ایم تا کاربران، برنامه‌های کدباز رایگان و در عین حال کارآمد را جایگزین نرم‌افزارهای موسوم به کینگ، لرد و... یا نرم‌افزارهای کرک شده یا قفل شکسته که غالبا آلوده به ویروس و بدافزار هستند، نمایند.

شماری از برنامه‌های کدباز، قابل حمل نیز هستند، یعنی شما می‌توانید این برنامه را روی یک فلش درایو با خود حمل کنید و در کامپیوترهای ناشناس به کار ببرید.

استفاده از برنامه‌های کد باز قابل حمل به امنیت بیشتر شما کمک می‌کند، چرا که:

- اگر تظیمات شما درست باشد، اثر و یا داده‌ای روی کامپیوتر میزبان به جای نمی‌گذارد.
- از استفاده از برنامه‌های نامطمئن و احتمالا آلوده کامپیوتر میزبان جلوگیری می‌شود.

در این بخش ساخت یک فلش درایو حاوی برنامه‌های پرتابل مورد نیاز را توضیح می دهیم.

قدم اول: یک فلش درایو ۲ یا ۴ گیگابایت را در کامپیوتر مطمئن خود فرمت کنید.

قدم دوم: آن را به شکلی که در بخش گذشته توضیح داده شد با Panda USB Vaccine واکسینه کنید.

قدم سوم: یکایک برنامه‌های پرتابل مورد نیاز خود را از مواردی که در پی می‌آید، دانلود و بر روی فلش درایو کپی کنید:

مرورگر قابل حمل Google Chrome[1]

با حجم بسیار کوچک می‌توانید مرورگر خود را همیشه همراه داشته باشید،این مرورگر طبعا پسوردهای شما را روی کامپیوتر میزبان ذخیره نمی‌کند، نکته قابل توجه اینکه اگر از گواهینامه‌های امنیتی خصوصی استفاده می‌کنید کروم گواهینامه شما را به لیست گواهی‌های تایید شده ویندوز کامپیوتر میزبان می‌افزاید، امری که برای کاربران عادی - مقدماتی چندان نگران‌کننده نیست.

مرورگر قابل حمل Firefox[2]

اگر به دلایلی امکان استفاده از کروم را ندارید، مثلا از افزونه‌ای برای عبور از فیلتر استفاده می‌کنید که تنها با مرورگر فایرفاکس سازگار است، می‌توانید مرورگر قابل حمل فایرفاکس را دانلود و روی فلش درایو خود نصب کنید.

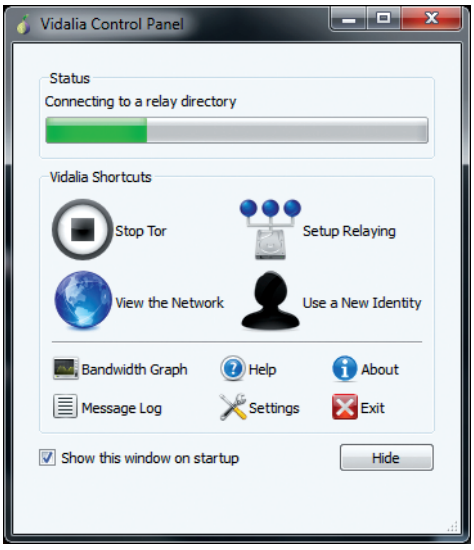
1. http://download.cnet.com/Google-Chrome-Portable
2. http://portableapps.com/apps/internet/firefox_portable

مرورگر قابل حمل Opera[1]

مرورگر اپرا نیز در سالهای اخیر به یکی از مرورگرهای مورد علاقه کاربران ایرانی بدل گشته است در آدرس سایت اپرا می توانید امکان نصب پرتابل این مرورگر را بیابید.

ناشناسی و عبور از فیلتر به وسیله Tor Browser Bundle[2]

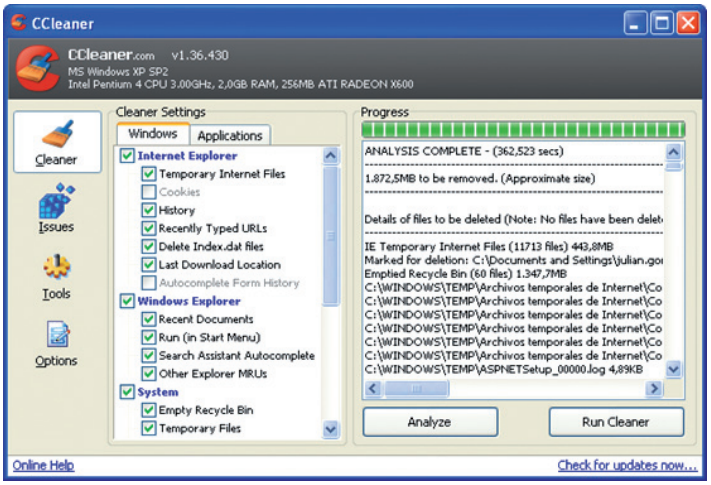
این نرم افزار تقریبا همه امکانات مرورگر فایرفاکس را در یک فایل فشرده یا زیپ، به علاوه امکان ایجاد ناشناسی و عبور از فیلتر توسط سرورهای پروژه تور را برای شما فراهم می آورد؛ نصب مرورگر تور بسیار ساده است کافی است از آدرس بالا مجموعه تور را در یک فایل فشرده حاوی برنامه نصب را دانلود و اجرا کنید.



1. http://www.opera.com/
2. https://www.torproject.org/about/overview.html.en

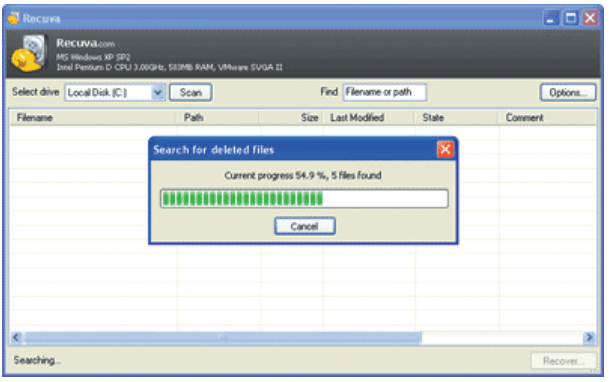
از بین بردن دائمی داده‌های غیرضروری به وسیله CCleaner[1]

این برنامه در بخش گذشته توضیح داده شد، آنچه اینجا مشاهده می‌کنید در حقیقت نسخه قابل حمل این برنامه است، مثلا می‌توانید این نسخه را در فلش درایو همراه خود به مدرسه، دانشگاه، کافی‌نت یا محل کار برده و قبل از ترک محل، همه آثار داده‌ها و کلا اطلاعاتی را که ممکن است سهوا در خلال کار شما با کامپیوتر میزبان به حافظه کمکی آن منتقل شده باشد، کاملا و برای همیشه غیرقابل بازیافت کنید. برای اطلاع بیشتر از نحوه کار این برنامه به بخش قبل مراجعه کنید.



بازیافت فایل‌های پاک شده به وسیله Recuva[2]

همانطور که در بخش گذشته توضیح داده شد، این برنامه رایگان به بازیافت فایل‌های پاک شده شما کمک می‌کند. نسخه قابل حمل این برنامه را می‌توانید برای مواقع ضروری همراه داشته باشید.



1. http://static.piriform.com/pf/download.png
2. http://www.piriform.com/recuva/download/portable

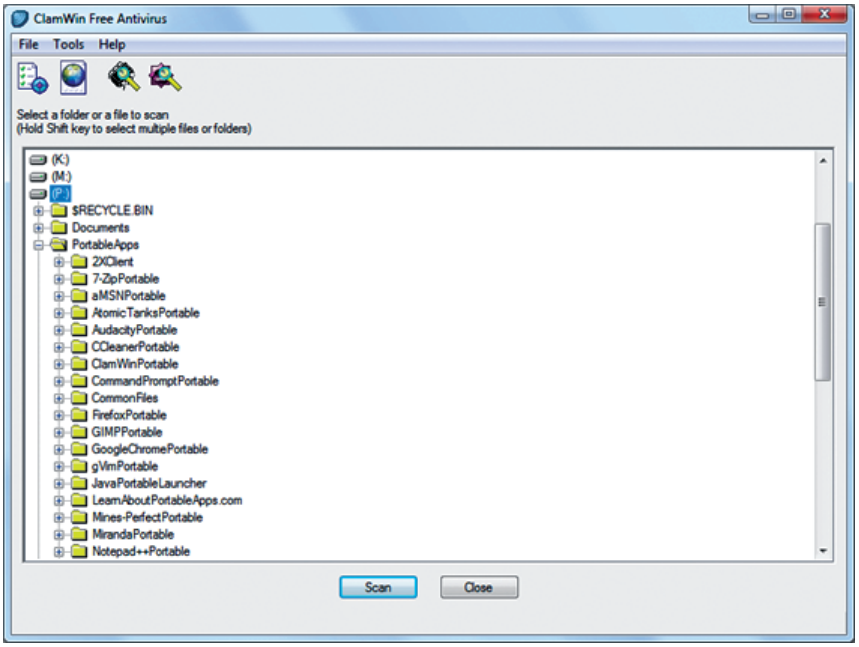
بازکردن فایل‌های فشرده شده به وسیله 7Zip[1]

این برنامه قادر است تقریبا همه فرمت‌های متفاوت فایل‌های فشرده شده را باز کند، در هنگام باز کردن فایل‌های فشرده، خصوصا فایل‌های فشرده شده با پسورد دقت کنید که قبل از اجرای برنامه‌ها تمام فایلها را اسکن نماید. هیچگاه از خود پرسیده‌اید چرا همه فایل‌های فشرده در وب‌سایت‌های ایرانی دانلود، پسورد دارند یا به صورت فشرده تو در تو هستند؟ دلیل این امر عموما ویروسی بودن این فایل‌هاست.

ClamWin[2]، آنتی‌ویروس روی فلش درایو

این آنتی‌ویروس قابل حمل روی فلش درایو برای اسکن، شناسایی و مقابله با ویروس‌ها به شما کمک می‌کند با این آنتی‌ویروس می‌توانید قبل از آغاز به کار با هر کامپیوتر ناشناس حافظه و هارد دیسک آن را کاملا به دنبال برنامه‌های مخرب جستجو کنید.

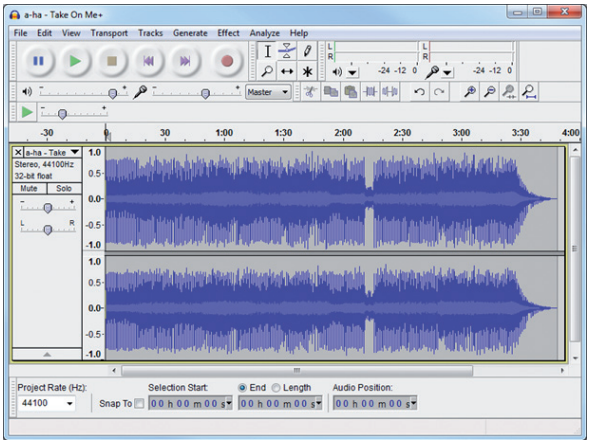
بسته‌های نرم‌افزاری متعددی شامل بعضا چندین آنتی‌ویروس برای استفاده روی فلش درایو معرفی شده‌اند و با جستجو در سایت‌هایی مثل http://portableapps.com می‌توانید هریک را آزمایش کنید.



1. http://www.7-zip.org/download.html
2. http://downloads.sourceforge.net/clamwin/clamwin-0.97.5-setup.exe

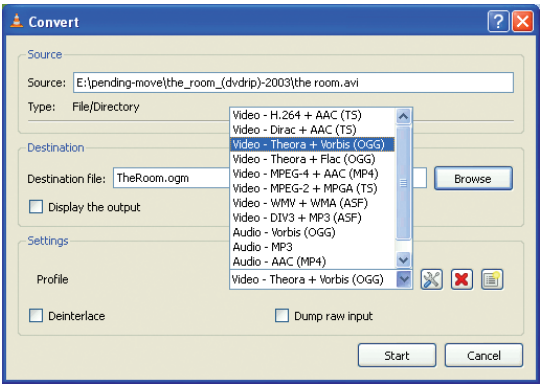
Audacity[1]، برنامه ضبط و ویرایش صدا

با این برنامه قدرتمند اما رایگان و قابل حمل می‌توانید از طریق میکروفن یا استریومیکس کامپیوتر خود، صدا ضبط کرده، این صدا را با موسیقی یا فایل‌های صوتی دیگر میکس کنید و سپس با فرمت دلخواه ذخیره نمائید. این برنامه می‌تواند مورد استفاده روزنامه‌نگاران و... برای ویرایش فایل‌های صوتی مصاحبه قرار گیرد.



VLC Player[2]

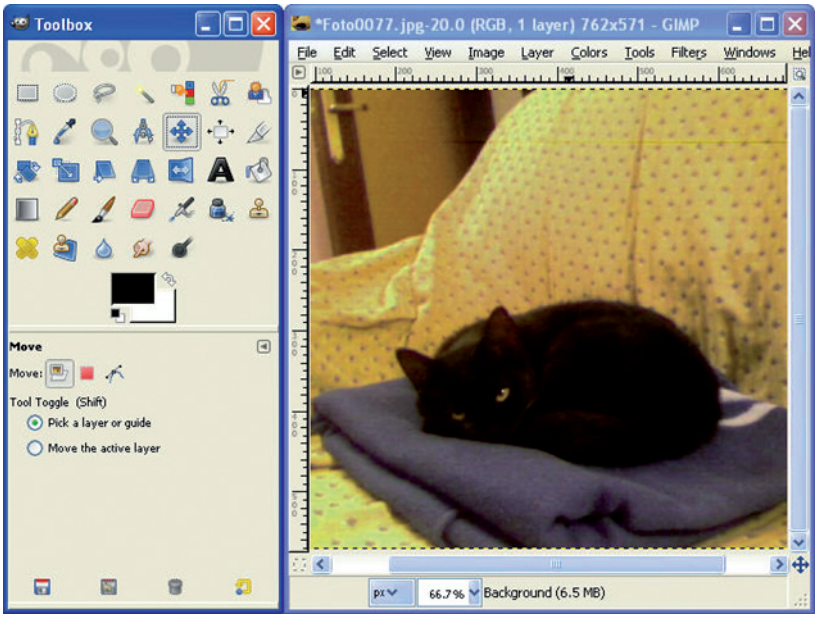
برنامه رایگان وی‌ال‌سی پلیر یکی از محبوب‌ترین برنامه‌های ویدئویی همه سال‌های اخیر است. این برنامه علاوه بر قدرت نمایش تقریبا همه فرمت‌های عمده ویدئویی به همراه زیرنویس قابل تنظیم، به شما امکان انتشار پدکست و ویدئوکست و همچنین تبدیل انواع مختلف ویدئو به یکدیگر را نیز می‌دهد. این برنامه را به سادگی می‌توانید روی یک فلش درایو به صورت قابل حمل نصب کنید.



1. http://audacity.sourceforge.net/download/windows
2. http://www.videolan.org/vlc/download-windows.html

GIMP[1]، جایگزین فتوشاپ

برنامه گیمپ بسیاری از امکانات نسبتا پیچیدهٔ برنامه ویرایش تصویر گران‌قیمت فتوشاپ را که مورد نیاز کاربر عادی و یا متوسط است، به رایگان در اختیار او قرار می‌دهد. با این برنامه می‌توانید عملیاتی مثل کوچک و بزرگ کردن عکس‌ها، چرخاندن، تغییر رنگ، سایه، فیلتر و تبدیل فرمت‌های مختلف گرافیک به یکدیگر را به سادگی مانند فتوشاپ انجام داده، نتیجه کار خود را ذخیره کنید.



Skype[2] قابل حمل

سایت portableapps نسخه قابل حملی از برنامه اسکایپ را برای دانلود رایگان منتشر نموده است. این نسخه می‌تواند از آسیبی که ممکن است در اثر وارد شدن با اسکایپ دیگران و برجای ماندن متن‌های چت شما ایجاد شود، جلوگیری کند. همچنین اطمینان خواهید داشت پسورد شما جایی ذخیره نخواهد شد. اسکایپ نرم‌افزار کدگذاری شدهٔ نسبتا امنی است که استفاده از آن در مکالمات ویدئویی و صوتی به کاربران ایرانی توصیه می‌شود.

1. http://portableapps.com/apps/graphics_pictures/gimp_portable
2. http://portableapps.com/apps/internet/skype_portable

مسنجر قابل حمل و مطمئن Pidgin[1] و افزونه OTR

سایت portableapps نسخه قابل حملی از برنامه پیدجین را نیز برای دانلود رایگان آماده نموده، این مسنجر پیدجین نام دارد و با اضافه کردن افزونهٔ OTR می‌تواند امنیت مکالمات چت متنی شما را بالا ببرد. پیدجین را روی کامپیوترهای ناشناس نصب نکنید، چرا که فایل متنی پسورد شما به راحتی توسط ادمین آن کامپیوتر قابل دسترسی است. افزونهٔ OTR مکالمات شما را در واقع محرمانه و غیرقابل ذخیره‌سازی می‌کند.

1. http://portableapps.com/apps/internet/pidgin_portable

http://www.tavaana.org

پروژهٔ

e-collaborative
for civic education

http://www.eciviced.org