" ضدتجسس " های

امنیتی

(روشهای ضد جاسوسی و ضد تفتیش در زندگی خصوصی)

توسط انجمن مبارزان سبز آزادی (ام سا)

شاخه‌ی ضدتجسس های امنیتی (ضد تا)

زمستان 1388

Contents

مقدمه:

هیچ کس تحت هر عنوانی حق تجسس و سرک کشیدن در زندگی خصوصی مردم را ندارد. هیچ کس در هر مقام و مسئولیتی اجازه ندارد آزادی های فردی و امنیت شخصی افراد را محدود و تهدید کند. چنانچه مراکز و سازمانهای امنیتی برای حفظ امنیت جامعه لازم است فردی را تحت نظر قرار گیرند، ضروری است مدارک و مجوز لازم را برای اینکار از مقامات ذی صلاح اخذ کنند و کارشان تحت نظارت مراکز دیگری که نماینده واقعی مردم است قرار داشته باشد.

در یک کشور آزاد که اطلاعات و اخبار ، شفاف و آزادانه گردش دارد چنانچه ، فرد یا گروه یا سازمانی بخواهد از موقعیت کاری خود سوء استفاده کند و وارد حریم خصوصی شهروندان شود، رسوا شده و از کارش جلوگیری میشود. اما متاسفانه در ایران چنین شفافیتی وجود ندارد. لذا ما با پدیده ای به نام اشرار امنیتی روبرو هستیم.

اشرار امنیتی به چه کسانی اطلاق می شود؟

افرادی که بالقوه دارای خصیصه های تبهکاری و شرارت هستند اما در موقعیت های امنیتی قرار میگیرند. این افراد، دارای حداقل رحم و شفقت هستند. مرئوسینی که به جای کلاه سر می آورند! به راحتی و به صرف وظیفه، هر گونه خشونت و جنایتی مرتکب میشوند.

آندسته از ماموران امنیتی که تبدیل به اشرار امنیتی میشوند دچار عقده عمیق و ریشه دار حقارت اند. افرادی ضد امنیت هستند که از آزار و ترساندن دیگران لذت میبرند. دارای اختلالات شخصیتی و اغلب سرخوردگی های شدید جنسی هستند. این امر از بازجویی ها ، شکنجه کردنها و شیوه های برخورد با زندانیان مستند به گزارشات و خاطرات ده ها زندانی مشهود است. از انجا که نام و وظیفه سازمانهای امنیتی ، به نوعی در مردم ایجاد رعب و وحشت میکند و اغلب افراد با احتیاط با آن روبرو میشوند، این گونه مراکز ، افرادی با خصوصیات ذکر شده را بشدت جذب خود میکنند زیرا ترسیدن دیگران از آنها و مانور قدرت دادن بویژه در فضایی غیر شفاف و غیر پاسخگو، عقده حقارت آنها را فرو مینشاند و از طرفی ارباب رجوعان خلع سلاح شده انها کسانی هستند مانند زندانی ها، شهروندانی که به هر دلیل تحت تعقیب قرار میگیرند و خانواده های این افراد که از موضع نابرابر برخوردارند.

سعید امامی و باند عملیاتی اش، بازجویان همسرش و عاملان جنایات کهریزک از این جمله اند که آشکار شده اند اما آیا به همین افراد ختم میشود؟

در کشور ما بخشهایی از مراکز امنیتی سالیان مدید است، دور از نظارت رسانه های مستقل و نمایندگان مردم در سایه و بطور پنهانی رشد سرطانی یافته اند. برای اشرار امنیتی حریم خصوصی و اطلاعات شخصی، واژگانی تعریف نشده اند. این اشرار به حریم شخصی هر که بخواهند سرک میکشند . در ظاهر قدرت های بلامنازعی هستند که گمان میکنند نامیرا و ابدی نیز هستند.

هدف اشرار امنیتی از شنود و تجسس چیست؟

وقتی با مراکز امنیتی روبرو هستید که عملکردشان هیچ خط قرمزی ندارد و نیز صرفا به اجرای قانون و پیگیری های قانونی نمیتوانید اکتفا کنید، لازم است که راه های مقابله با این گونه اشرار را یاد بگیرید و توان مقابله با این دزدی ها و تجسس های غیر قانونی را در خود بالا ببرید. چون از هر اطلاعاتی که از شما یافت میشود علیه شما و به قصد سرکوب شما استفاده میشود.

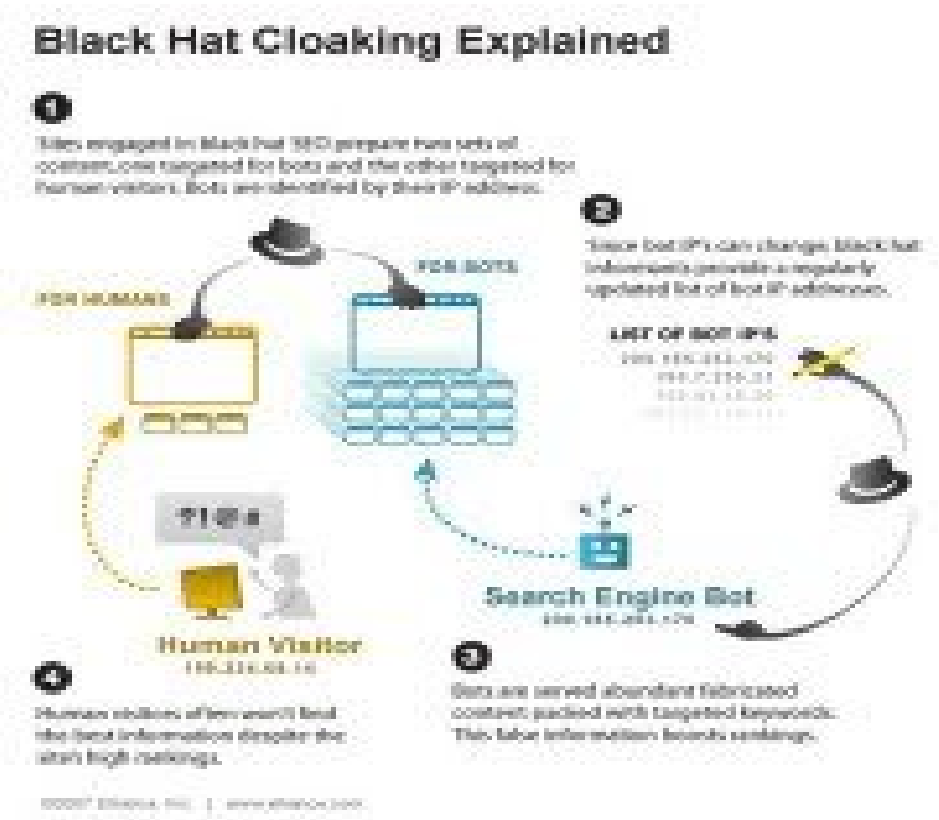
اشرار امنیتی به این دلیل در حریم خصوصی افراد سرک میکشند تا نقطه ضعفی بیابند یا چیزی را تبدیل به نقطه ضعف کنند و علیه افراد بکار گیرند. بخصوص در مورد خواص یا مسئولین مملکتی و خانواده نزدیک آنها با هدف باج خواهی، حق السکوت، وادار کردن به اظهار نظر یا سکوت اجباری و یا تخریب و ترور شخصیت اقدام به تهیه پرونده های ویژه ای در این ارتباط میکنند. بعنوان نمونه فیلم هایی از روابط بسیار خصوصی افراد بطور پنهانی و با سوءاستفاده از ابزار جاسوسی تهیه کرده و در مواقعی که پروژه تخریب آن اشخاص کلید میخورد یا برای انحراف افکار عموم از مساله ای حاد ،بطور ناگهانی منتشر میکنند. فیلم مربوط به رابطه جنسی امام جمعه تویسرکان نمونه ای از این دست بود. گفته می شود فیلم رابطه جنسی هنرپیشه جوان تلویزیونی نیز در موقعی خاص برای انحراف افکار عمومی از مساله ای بود که همزمان جریان داشت.

لذا این مجموعه بصورت کاملا کاربردی به روشنگری درباره روشهای دزدی اطلاعات و تجاوز به حریم خصوصی افراد می پردازد تا لااقل شهروندان ایرانی بویژه جوانان و دانشجویان بتوانند در مواجهه با این دزدان امنیتی در حد ممکن از حریم خصوصی خود دفاع کنند. مواردی که در این مجموعه طرح میشود شامل موارد علمی و مسلم تا احتمالات و از ساده ترین و عمومی ترین نکات تا نکاتی است که برای افراد خاص و بشدت تحت نظر قابل استفاده است. لزوما افراد عادی نیازی به رعایت همه این نکات ضد تجسس ندارند اما آگاهی به وجود روشهای مختلف دزدی اطلاعات و جاسوسی و امکان سوء استفاده از آنها به حفظ امنیت حریم شخصی کمک بسیار مینماید.

همچنین ذکر این نکته ضروری است که بسیاری از این روشها، از روشهای سوخته اطلاعاتی و امنیتی است و احتمال دارد برای ضد شنود ها ، ضد ضد شنود هم بکار رود اما آگاهی نسبت به همین روشها سبب میشود هوشیاری نسبت به دزدی ها و تجسسات اطلاعاتی و امنیتی افزایش یابد که خود نقشی تعیین کننده در خنثی سازی دزدی های اطلاعاتی دارد و علاوه بر آن تجربه نشان داده که بکارگیری این نکات ایمنی تا حدود بسیار زیاد و موثری موجب حفظ حریم خصوصی و کوتاه شدن دست اشرار امنیتی می شود.

فصل اول:

امنیت رایانه و روشهای دزدی اطلاعات



رایانه برای اغلب ما وسیله ای است چند منظوره: آلبوم عکس، آرشیو فیلم،کتابخانه ، گنجینه مطالب خصوصی، دفتر عقاید و اندیشه(وبلاگ)، محل قرار ها و ملاقاتها(فیس بوک، مسنجرها) و به عبارتی مخزن همه اطلاعات کاری، شخصی و محرمانه. به همین دلیل در بازداشت افراد اولین چیزی که ضبط میشود، کامپیوتر شخصی انهاست. زیرا هارد کامپیوتر گفته های زیادی برای بازجویان دارد حتی چیزهایی که در حافظه شما نیست. در عین حال همه اطلاعات شخصی و خصوصی شما را بدون اجازه و خواست شما در دسترس قرار میدهد.

"همان شب بازجوها رفته بودند در ِ خانه مان و کیس کامپیوترم را توقیف کرده بودند. از روز بعد، باید می نشستم درباره ی پوشه هایی که در حافظه ی کامپیوترم ذخیره بود، توضیح می دادم. نامه ها، عکس ها، پوشه های صوتی و تصویری، ID ها، نشانه ها، علامت ها، آدرس ها، همه

و همه، حتی نامه های خصوصی ام به آقا و خانم فلانی، عکس های خصوصی ام، همه را دیدند، به رابطه های خصوصی ام پی بردند، زندگی ام را زیر و رو کردند تا به اقدام های پنهان مانده شده بر علیه حکومت شان پی ببرند!" [1]

از جمله روش های تجسس و نفوذ به اطلاعات رایانه میتوان به این موارد اشاره کرد:

- اطلاعات هارد کامپیوتر تا هفت بار format نیز قابل بازیافت است.
- اتصال به اینترنت یا وصل دائم خط تلفن به رایانه راهی برای ورود بدون اجازه به داخل کامپیوتر است.
- میشود از طریق خطوط برق و رایانه متصل به برق اطلاعات داخل کامپیوتر را دزدید. البته چنین روشهایی برای سوژه های خاص مورد استفاده قرار میگیرد.۲
- برخی ویروسهای کامپیوتری برای هک کردن و دزدی اطلاعات ساخته شده اند و با ورود به رایانه از فایلها کپی میگیرند و در اولین فرصت که رایانه به اینترنت وصل شد آن اطلاعات را به آدرس مشخصی ارسال میکنند.
- از طریق کامپیوتر که دارای وب کم باشد (مانند نوت بوکهای جدید) با اتصال به اینترنت امکان نفوذ و جاسوسی تصویری و شنیداری وجود دارد.

توصیه ها ی امنیتی

در مقابل روشهایی برای افزایش امنیت اطلاعات و رایانه وجود دارد که عبارتند از:

1-استفاده از فلش مموری(کول دیسک) ، memory stick, sd و هارد اکسترنال برای مطالب و فایلهای محرمانه.

2-هارد اکسترنال برای فایلهای بشدت محرمانه ابدا توصیه نمیشود. هارد اکسترنال به دلیل ظرفیت بالاتر از فلش، برای تهیه فیلم و بلوتوث میتواند بکار رود.

---

[1] .از خاطرات زندان کیانوش سنجری

[2] . **سرقت اطلاعات از طریق شنود صدای تایپ بر روی صفحه کلید رایانه**

به گفته پژوهشگران در امر امنیت اطلاعات، از پریز برق می توان برای شنود آنچه مردم بر روی صفحه کلید رایانه تایپ می کنند، استفاده کرد.

پژوهشگران موسسه Inverse Path دریافته اند که فقدان لایه های حفاظتی کافی جهت جلوگیری از انتشار اعوجاج در کابل برخی صفحه کلیدها، باعث می شود که در هنگام تایپ هر حرف، اطلاعاتی حساس از طریق این سیم نشت کند. این پژوهشگران با تحلیل اطلاعاتی که از طریق پریز برق به دست آمد، توانستند دریابند که فرد مورد شنود قرار گرفته، چه چیزی بر روی صفحه کلید کامپیوتر خود تایپ می کند.

در این پژوهش مشخص شد اطلاعات منتقل شده از طریق سیم صفحه کلید، از 15 متری نقطه اتصال رایانه به یک پریز برق و حتی از نقاطی مانند لوله های آب نیز قابل شنود است. (منبع ایسنا)

3-ذخیره عکس و مطالب خصوصی و شخصی مانند عکس و فیلم های خانوادگی برروی دی وی دی یا هارد اکسترنال.

4-نصب نرم افزارهای امنیتی windows washer و Security Delete برای حذف کامل اطلاعات از روی هارد.[3]

5-استفاده از رمز برای ورود به رایانه . رمز گذاری بر روی فایل ها.

6-اطمینان از خالی بودن سطل زباله رایانه.

7. استفاده از برنامه هایی مثل nero برای رایت کردن روی cd یا dvd زیرا گفته میشود که رایت با ویندوز سبب میشود یک نسخه از فایل مورد نظر در هارد کامپیوتر باقی بماند.

توصیه های فوق امنیتی:

1-تعویض هارد کامپیوتر با هارد نو و دست اول یا هاردی که صاحب قبلی آن را میشناسید.

(نوت بوکها نیز قابلیت تعویض هارد دارند.)

2-در هنگام وصل شدن به اینترنت، مطمئن شوید که هارد اکسترنال یا فلش مموری به کامپیوتر وصل نیست.چون احتمال دارد خط تلفن شما تحت کنترل باشد.

3-استفاده از نوت بوک بدون اتصال به برق. راه ساده دیگر ، استقرار در مکانی امن و ردیابی نشده است.

4-رمز قوی روی همه فایلهای حساس. رمز باید شامل حرف و عدد باشد و ترجیحا از دوازده رقم و بیشتر برای رمز فایلها استفاده کنید.بخصوص برای ایمیل و فایلهای حساس و محتوای اطلاعات بسیار خصوصی زیرا با وجود نرم افزارهای کشف رمز ، عدد به تنهایی یا حرف به تنهایی و یا تعداد ارقام کم رمز ، به سهولت انجام میپذیرد. همچنین از اسم و اعداد مربوط به خود مانند تاریخ تولد یا شماره شناسنامه و مواردی از این دست برای رمز گذاری استفاده نکنید.

5- غیر فعال کردن حافظه Hibernate

به این ترتیب اقدام کنید.

دکمه start ← control panel ← قسمت power option ← انتخاب صفحه hibernate ← مربع کنار enable Hibernate را بدون تیک کنید.

[3]. در انتهای این فصل به معرفی برخی از این برنامه ها میپردازیم.

6- پاک سازی فضای رزرو توسط clean up :

نکته: بعضی اوقات بعد از خالی کردن سطل آشغال هم فضای رزور دیسک پاک نمیشود و راهش clean up است.

روی حرف نشاندهنده دیسک مورد نظر در windows Explorer کلیک کنید. ← انتخاب گزینه properties ← انتخاب دکمه disk cleanup

7- پاکسازی پس از disk cleanup:

Disk cleanup فقط فایلهای موقتی ماقبل هفته آخر را پاک میکند. برای پاک کردن فایلهای موقتی جدیدتر این قدمها را دنبال کنید

کلید start ← انتخاب Run ← تایپ عبارت temp ← محتوای فولدر باز شده را انتخاب کرده و حذف کنید.

8- پاکسازی حافظه مجازی :

حافظه مجازی قسمتی از حافظه دیسک سخته که به صورت موقت در اختیار سیستم عامل قرار میگیره. ویندوز از این فضا برای نگهداری داده های موقت خودش استفاده میکنه. مقدار پیش فرض این حافظه که توسط ویندوز تعیین میشه بهترین انتخابه و به ندرت پیش میاد که کسی بخواد اونو تغییر بده. در صورتی که کسی به خاطر کمبود فضای دیسک سخت، میزان حافظه مجازیش رو کاهش بده، مسلماً با افت سرعت سیستم مواجه میشه. همچنین کسی که اونو به حداکثر برسونه باعث میشه فضای بیشتری از دیسک در اختیار سیستم عامل قرار بگیره که مدیریت اون، باز هم موجب کاهش سرعت میشه.

برای افزایش یا کاهش حافظه مجازی مراحل زیر و دنبال کنید :

- روی My Computer راست کلیک کنید و Properties رو انتخاب کنید.
- در پنجره ای که ظاهر میشه (System Properties) برگه Advanced رو انتخاب کنید و در قسمت Performance روی Settings کلیک کنید.
- در این پنجره (Performance Option) برگه Advanced رو انتخاب کنید و در قسمت Virtual Memory روی دکمه Change کلیک کنید.
- در پنجره ظاهر شده (Virtual Memory) در قسمت Paging file size for selected drive روی Custome size کلیک کنید، حالا در کادر جلوی Initial size (MB) فضای دلخواهتون رو بر حسب مگا بایت تعیین کنید و روی دکمه Set کلیک کنید و سپس روی OK کلیک کنید تا تغییرات اعمال بشه.

{بعد از آزاد شدن حافظه مجازی لازم است توسط نرم افزارهایی که میتوانند فضای خالی هارد دیسک را پاکسازی و غیرقابل بازیافت کنند ، پاک شود. (مثل O&O) }

8- پاک کردن دستی لینکهایی که برنامه های ویندوز میسازند و در فولدرهایی بنام RECENT ذخیره میکنند.

معمولا بیش از یک RECNET بروی درایوی که ویندوز نصب است وجود دارد. (خصوصا در مسیرهایی که OFFICE وجود دارد)

استفاده از برنامه های پاک کننده قسمتهای گوناگون هارد. مثل

WINDOOWS WASHER. WASH &GO . TRACK ERASER PRO....

هر کدام از این برنامه ها قابلیتهای ویژه خود را دارد. بنابراین نصب بیش از یکی از این برنامه ها روی دستگاه مناسب است.

9- استفاده از برنامه های پاک کننده ضدبازیافت. فعلا بهترین برنامه دراین زمینه O&O SAFE ERASE شناخته شده است.

10- استفاده از چند روش برای حذف فایل ها از روی هارد کامپیوتر. به این ترتیب که :

ابتدا محتویات فایل را با مطالب کم اهمیت جایگزین کنید، نام فایل را تغییر دهید و سپس فایل تغییر یافته را با نرم افزار ضد بازیافت ، حذف کنید.

شنود و جاسوسی در فضای مجازی (اینترنت)

گفته شده ایران از تکنولوژی DPI (Deep Packet Inspection) برای شنود اینترنت برخوردار است. چنان چه این درست باشد به این مفهوم است که تجهیزات شنود می توانند همه گونه بسته های اطلاعاتی که در اینترنت رد و بدل میشود را بگشایند. راه مقابله با آن استفاده از فیلترشکن های VPN-based است، اگر تجهیزات شنود بسته ها را بگشایند، قادر به تشخیص محتوای آنها نخواهند بود. البته غیر از این در محیط اینترنت ویروسهای جاسوس و شنودگر هم وجود دارد.۴ غیر از اینها هکر ها و نرم افزارهای جاسوسی مختلفی وجود دارند که دزدانه وارد رایانه یا پست الکترونیک شما میشوند.

"... چیزی که باعث شد مات و مبهوت بمانم، این بود که متن چاپ شده ی برخی از ایمیل هایم را گذاشتند جلوم و پیرامون آنچه نوشته بودم توضیح خواستند. البته پیش از بازداشت شدن، متوجه شده بودم که ID ام در Yahoo هک شده بود. چون عنوان های نامه هایم خاکستری بود. یعنی یک نفر پیش از من نامه هایم را خوانده بود. به همین خاطر بود که دیگر از ایمیل ام در Yahoo استفاده نمی کردم. اما نامه هایم در Gmail سالم و دست نخورده بودند. تا به حال پیش نیامده بود که Gmail ام را باز کنم و متوجه بشوم که نامه هایم خوانده شده باشد. حدس می زدنم آن ها با راه یافتن به مسیر مودم کامپیوترم، به شبکه ی اینترنت ام دسترسی پیدا کرده بودند. این کار آسانی است. کافی ست از شرکت ارائه دهنده ی اینترنت (که در اختیار دولت است) بخواهند که مشترکی که با فلان شماره ی تلفن به اینترنت متصل می شود را زیر نظر داشته باشند. آن ها از این طریق، یا از هر طریقی که من نمی دانم، توانسته بودند هر صفحه ی Explorer ای که من در خانه گشوده و دیده بودم را ببینند و چاپ کنند. مثلا یک بار یک صفحه ی اینترنتی با عکس هایی از عیسی مسیح که بر صلیب آویزان بود را جلوم گذاشتند تا درباره اش توضیح بدهم. آن ها می خواستند بدانند که آیا من مسیحی شده بودم!." [5]

---

[4] .**شناسایی ویروس شنودگر.** محققان امنیتی کد حمله ای را که در اینترنت انتشار یافته و قادر است مکالمات صوتی و ویدیویی انجام گرفته از طریق برنامه تلفن اینترنتی (voip) اسکایپ را شنود کند، شناسایی کردند.
به گزارش ایسنا این تروژان که skype.peskyspyنام دارد مکالمات را در رایانه ای که آلوده کرده پیش از رمزنگاری و ارسال شدن آن ها در شبکه ضبط و به شکل فایل mp3 ذخیره می کند تا بعدا آن ها را منتقل کند.
با این که اسکایپ داده ها را هنگام انتقال بین تماس گیرندگان محافظت می کند اما این تروژان می تواند در نقطه دریافت یا ارسال اطلاعات را رهگیری کند.
این نرم افزار مخرب از طریق لینک های ایمیل و ترفندهای مهندسی امنیتی به کار بسته شده در هرزنامه ها و پیام ها منتشر شده است .

[5] . از خاطرات زندان کیانوش سنجری

توصیه هایی برای مقابله با شنودها و جاسوسی ها و ردیابی های اینترنتی:

1-نصب آنتی ویروس قوی دارای اینترنت سکیوریتی بر روی کامپیوتر شخصی میتواند تا حد بسیار زیادی از ورود هر گونه نرم افزار جاسوسی و مزاحم جلوگیری کند.

2-رمز گذاری روی فایلهایی که میخواهید از طریق ایمیل رد و بدل کنید.

3-هر فیلتر شکنی قابل اعتماد نیست!

هر ابزاری که به شما اجازه رد کردن فیلتر را بدهد لزوما امن نیست چرا که رد تمامی فعالیت هایی که یک کاربر با استفاده از یک فیلترشکن انجام داده در Log آن فیلترشکن باقی خواهد ماند و این لاگ یا به صورت رمز نشده است و اگر هم رمز شده باشد روش Decipheringآن و کلید مورد استفاده اش معمولا بطور باز در همان نصب محلی وجود دارد.

عدم استفاده از هر VPN ای

با وجود آنکه وی پی ان ها روش بسیار بهتر و کامل تری نسبت به فیلترشکن های وبی می باشند و عموما در مواردی همچون نمایش ویدئو و اجرای جاوا اسکریپت های صفحات وب اختلال ایجاد نمی کنند، بازهم دلیل نمی شود که هر وی پی ان ای را مورد استفاده قرار دهیم. به عنوان مثال اگر می بینیم که سایت های ایرانی فیلترینگ در اینترنت آزادانه و برای مدت طولانی در حال فروش اکانت های وی پی ان هستند و دارای شماره تلفن و شماره حساب می باشند، بدنیست کمی نسبت به این موضوع بدبین باشیم چون وی پی ان چیزی نیست که بتوان به سادگی و آزادنه آن را به فروش رساند .اصولا وی پی ان های گمنام یا تهیه شده از افراد معتمد بهتر از وی پی ان هایی است که برای مدت طولانی با درج نام شرکت و شماره حساب و شماره تلفن های ثابت به فروش می رسند.

4- HTTPS - بجایHTTP

اگر در هر وب سایتی دیدید از HTTPS استفاده شده است یا دیدید که امکان استفاده SECURE دارد حتما از آن استفاده کنید. می توانید خودتان دستی تست کنید که آیا با اضافه کردن S باز هم سایت آیا قابل استفاده است یا خیر .این موضوع در ارسال ایمیل، استفاده از سرویس های پیام رسانی وبی مثل تویتر و امثالهم که شما فقط بیننده نیستید و خودتان هم تعامل با سایت دارید نمود بیشتری دارد.

5-فیلترشکن های توزیع شده

برخی فیلترشکن ها بر پایه VPN توزیع شده و جز به جز (Peer-To-Peer) وجود دارند که امنیت بسیار بالایی را فراهم می کنند. این فیلترشکن ها جزء بهترین راهکارهای گردش در اینترنت محسوب می شوند و از آن میان می توان به OpenVPN و TOR اشاره نمود. FreeGate و UltraSurf نیز اطمینان بالایی دارند و اینگونه ابزارها می توانند بصورت مطمئن بکار روند. اخیرا cproxy و usejump نیز بعنوان فیلتر شکن قابل استفاده اند.

6-عدم استفاده از مسنجرهایی که ارتباطات را بدون رمز ارسال می کنند.

اثبات شده که مسنجرهای مایکروسافت مانند MSN و Live به گونه ای تبادل اطلاعات می کنند که با Deep Packet Inspection قابل شنود هستند. استفاده از این ابزارها را کلا کنار بگذارید و به مسنجر های امن اعتماد کنید. ضمنا با استفاده از ابزارهایی مثل سیمپلایت برای یاهو مسنجر می توانید یاهو مسنجر خود را در مقابل جاسوسی امن تر کنید.

7-ایمیل های رمز شده و پسوردهای قوی.

با وجود اینکه اکنون ایمیل هایی مانند aol و gmail امنیت خوبی را در ارسال و دریافت بخصوص با (HTTPS) نشان می دهند می توانید از ایمیل های رایگانی همچون هوش میل (Hushmail) که ایمیل رایگان با قابلیت رمزنگاری توسط کاربر را ارائه می دهند استفاده کنید.

ایمیل خود را با نام کامل خود نسازید. همچنین از پسوردهای قوی (ارقام بالا و شامل حرف،عدد، علامت) برای ایمیل کمک بگیرید.

8-عدم استفاده از نام واقعی خود و استفاده از نام مستعار

نه تنها از نام خود استفاده نکنید بلکه از تنها یک نام مستعار هم استفاده نکنید. حتی از نام های مستعار خیلی منحصر به فرد هم استفاده نکنید. سعی کنید از شماره های ردگم کن برای انتهای نام مستعار خود استفاده کنید

Computer Name خود را به هیچ وجه هم اسم خود یا نامی مرتبط با خود انتخاب نکنید.

از آنجایی که در HTTP Headers هر وب سایتی به صراحت نام کامپیوتر شما می افتد به هیچ وجه نام کامپیوتر خود را همنام خود یا حتی نام های مستعارتان برنگزینید. نام های عمومی مثل HOME می توانند بسیار خوب باشند.

هنگام نصب نرم افزارها در کامپیوتر خود به هیچ وجه با نام خودتان رجیستر نکنید.

فایل هایی که با برخی نرم افزارها مانند ورد (فایل های متنی) و فتوشاپ (تصاویر)، پی دی اف و امثالهم درست می شوند با خود اطلاعات سازنده یا نویسنده فایل (Author)را نگهداری می کنند و بعد از چندین بار دست به دست شدن هم باز نام نویسنده اصلی فایل بر روی آنها باقی می ماند. بنابراین به هیچ وجه موقع نصب برنامه ها نام اصلی خودتان را برای رجیستر کردن استفاده نکنید.

9-از فیلتر شکن نه فقط برای باز کردن سایتهای فیلتر شده بلکه برای تغییر ip خود نیز استفاده کنید.حتی در کافی نت. میتوانید با سرچ my address ip در گوگل متوجه شوید که ip شما تغییر کرده است یا نه؟

توصیه های فوق امنیتی:

1-اگر احتمال میدهید خط تلفن شما تحت کنترل است، در هنگام وصل شدن به اینترنت، مطمئن شوید که هارد اکسترنال یا فلش مموری حاوی مطالب خصوصی و حساس به کامپیوتر وصل نیست.

2-برای آپلود و ارسال مطالب و فایل های حساس مانند فیلم هرگز از کامپیوتر شخصی و یا از منزل یا محل کار و یا دانشگاه آپلود نکنید. کافی نت ها مطمئن تر از جاهای دیگر است.

3-در صورتیکه سایتها و وبلاگهای حساس را آپ میکنید، هنگام کار در کافی نت، ترجیحا با تغییر لباس و مدل مو و کلاه و عینک و ... ظاهر خود را متفاوت از وقت معمول کنید. (ممکن است به دوربین مجهز باشند)

4-با احتمال روشن بودن وب کم کامپیوتر ها در کافی نت ها و ضبط فیلم از شما بدون آنکه متوجه باشید، وب کم را قبل از قرار گرفتن پشت دستگاه بچرخانید.

5- با ارسال مطالب به دوستان و آشنایانی که در خارج از کشور دارید از انها بخواهید فایل شما را در وب آپلود کنند.

6- همیشه از یک کافی نت استفاده نکنید.

7-بعد از پایان کار و قبل از بلند شدن از پشت کامپیوتر در پنجره اکسپلورل اینترنت از طریق tools

Internet optins ,

و general

و setting

history آن را از سایتهایی را که رفته اید پاک کنید.

میتوایند از دسیک کلین آپ disk clean up هم استفاده کنید.

8-ایجاد ایمیل با نام های مستعار از خطوط تلفنی ایمن از نظر کنترل و تعویض ایمیل ها هر چند وقت یکبار یکی از بهترین راه های بالا بردن حفاظت از هکرهاست.

***مهمترین توصیه ما به شما:**

1. استفاده از فیلتر شکن یا پراکسی هایی که هویت و ip شما را تغییر داده و مانع شناسایی محل و موقعیت شما میشوند.

2. عدم استفاده از اینترنت منزل یا محل کار و تحصیل برای کاربردهای حساس

از جمله این پراکسی ها:

- سی پراکسی
- سای فان
- یوزجامپ

....

معرفی کتاب:

" پیشگیری از سرقت اطلاعات رایانه ای "

نویسنده : سید پاشا ناصرآبادی

کتاب "پیشگیری از سرقت اطلاعات رایانه ای" به عنوان مرجع جدید دوره ی آموزشی " امنیت اطلاعات رایانه ای" معرفی شده است . این کتاب که توسط سید پاشا ناصرآبادی تالیف شده است به بررسی روش های ساده پیشگیری از سرقت اطلاعات رایانه ای کاربران می پردازد .

فصل دوم:

شنود و ضد شنود

"می پرسه وقتی آزاد بشی در مورد زندان چی می نویسی؟ میگم: از تهدید، بازجویی، شکنجه روانی، تحقیر و برخوردهای بد شما و وضعیت بد زندان .... و مرد میگه حتما می نویسی که مسائلی رو از زندگی ات مطرح کردیم که با شنیدنش، تا مدتی نمی تونستی حرف بزنی.... و من میگم کار مهمی نیست شنود تلفن دیگران ....."[6]

شنود، شیوه های مختلف و ابزار متنوعی دارد. از شنود تلفنی تا نصب ابزار ظریف و بسیار کوچکی که در مکانهای مختلف تعبیه میشود و به شنود گفتگوها میپردازد. ممکن است الکتریکی باشد و با باطری کار کند یا اینکه لیزری باشد. ممکن است برد کوتاهی داشته باشد یا اینکه تا چند کیلومتر از مرکز کنترل فاصله داشته باشد. حتما نباید نزدیک محل شنود یک ون با شیشه های تیره و مشکوک وجود داشته باشد! حتی ممکن است ابزاری بسیار ریز و چسبنده باشد که به لباس یا کفش سوژه میچسبد و تا برد چند کیلومتری هم میتواند کار کند.

توصیه های فوق امنیتی ضد شنود حضوری(غیر از تلفن):

1. تغییر مکان دادن.
2. گذاشتن لباس رو و کیف و کفش در اتاق دیگر یا درون کمد.
3. به زبان نیاوردن کلمات حساس . یا بنویسید یا لب خوانی کنید.
4. استفاده از یک داستان یا سناریو برای بیان آنچه میخواهید بگویید. مثلا در قالب تعریف یک فیلم داستانی.
5. قال گذاشتن شنودگر: در مکانهایی که به احتمال بسیار زیاد شنود می شود گفتن مطالبی به عمد و برای به اشتباه انداختن شنود گر و انحراف توجه او. مثلا قرار ملاقات فرضی گذاشتن در مکانی دیگر ولی به جای دیگری رفتن.
6. استفاده از رمزو نام مستعار برای مکانها و ساعات قرار و افراد

[6] از خاطرات زندان محبوبه حسین زاده

(توجه داشته باشید: بازکردن شیر آب و ایجاد سر و صدا هم فایده چندانی ندارد چون امکان فیلتر کردن صداها بر حسب ارتعاش وجود دارد.)

شنود و ضد شنود تلفنی

امروزه هر جا سخن از استراق سمع و شنود مکالمات تلفن های همراه به میان می آید تصویری که در اذهان عامه نقش می بندد این است که در هنگام برقراری تماس ، مکالمات رد و بدل شده توسط دستگاهی واسط ضبط می شود و مورد شنود قرار می گیرد.

شنود تلفنی به معنای این است که ارگان امنیتی و اطلاعاتی، در صورتی که نیاز این کار را به هر دلیلی تشخیص دهد، امکان این را داشته باشد که شماره آن تلفن همراه را زیر نظر قرار دهد. به بیان گسترده تر، همه مکالمه ها، پیامک های نوشتاری (SMS) و تصویری (MMS)، ارتباط با اینترنت (GPRS) که به آن شماره می رسند و یا از آن فرستاده می شوند، مورد شنود قرار می گیرند.

این نوع استراق سمع اگر چه می تواند مورد استفاده قرار گیرد اما با پیدایش تلفن های همراه و گسترش ارتباطات سیار ، شیوه های جدید و کاراتری جهت شنود مکالمات و استراق سمع های محیطی به کار گرفته می شود.

شنود از طریق تلفن های همراه

تلفن همراه از دو بخش اساسی سیم کارت و گوشی تشکیل شده است که از هر دو ناحیه تهدید پذیر و یا به عبارت دیگر قابل شنود می باشد.

از طریق سیم کارت میتوان شنود و ردیابی کرد و با استفاده ازگوشی، نرم افزار شنود و انتقال اطلاعات به صورت خودکار صورت میگیرد.

روشهای شنود و ردیابی از طریق تلفن همراه:

1-تغییرات سخت افزاری و نرم افزاری .

به وسیله تغییرات سخت افزاری و نرم افزاری که در گوشی های موبایل انجام می دهند این گوشی ها بدون اینکه صاحب آنها متوجه باشند روشن می شود و اطلاعات با ارزشی را به جاسوسان می رساند.

2-شنود از طریق میکروفن گوشی.

3-برنامه ریزی یک شماره خاص در گوشی:

یعنی شماره فرد شنود کننده در گوشی فرد شنود شونده با نرم افزار خاص طوری تنظیم می شود که وقتی فرد جاسوس با شخص مورد نظر تماس می گیرد، گوشی زنگ نمی خورد ولی میکروفون دهنی آن روشن می شود و جاسوس می تواند شنود را انجام دهد.

4-روش switched off (شنود پس از خاموش شدن گوشی توسط سوژه):

یعنی پس از خاموش کردن گوشی توسط کاربر احتمال شنود وجود دارد. بعد از خاموش شدن صفحه نمایش به صورت خودکار اقدام به شماره گیری عناصر شنود کننده که قبلا در حفره های نرم افزاری ثبت شده است می نماید. سپس با برقراری ارتباط، به فرستنده ای مخفی برای شنود تبدیل می شود.

توجه: درآوردن باطری نمی تواند یک راهکار برای جلوگیری از جاسوسی باشد چون ممکن است باطری کوچک قابل شارژی قبلا در مدارات آن تعبیه کرده باشند.

5-روش دو سیم کارته کردن گوشی:

در این روش یک سیم کارت ثانویه همراه با یک سخت افزار کوچک جانبی در گوشی جاسازی می شود که این سیم کارت می تواند واقعی یا کپی یک سیم کارت باشد. در این روش در صورت تماس با سیم کارت دوم، گوشی روشن می شود بدون اینکه هیچ گونه علامتی نشان داده شود و به این ترتیب عملیات شنود بدون اطلاع سوژه انجام می شود.

6- smsها و بلوتوث های جاسوس

برای فعال کردن سیستم شنود و جاسوسی، عموماً نیاز به نصب نرم افزار مربوطه بر روی تلفن همراه افراد قربانی است که این عمل ممکن است از طریق ارسال پیامک و بلوتوث انجام گیرد. در صورتی که فرد مهاجم بخواهد از شیوه ارسال پیامک برای نصب این نرم افزار مخفی استفاده نماید ، پیامکی عمومی مانند تبریک سال نو به طیف وسیعی از مشترکان یک شهر ارسال می کند و مشترکان تلفن های همراه نیز پس از خواندن این پیامک ، فرد مهاجم را در جایگذاری این جاسوس کوچک یاری می رسانند!
لازم به ذکر است که این سیستم جاسوسی ، تنها محدود به شنود مکالمات محیطی نمی شود بلکه این دستگاه ها قادر به دسترسی به تمامی بخش های تلفن همراه از قبیل یادداشت های شخصی ، پیام های کوتاه ، لیست تماس ها و ... نیز می باشند.

7-روش استفاده از حفره های نرم افزاری بدون وابستگی به شماره تلفن و با شماره گیری خاص در تلفن های دو منظوره:

Spy phone ها گوشی هایی هستند که دارای دو وضعیت می باشند. در وضعیت عادی به طور معمول انجام وظیفه می کنند ولی در وضعیت جاسوسی به گونه دیگری عمل می کنند در این حالت شماره ای در گوشی برنامه ریزی شده و همچنین در حفره های نرم افزاری این گونه تعریف شده که به محض اینکه از شماره جاسوس با این گوشی تماس گرفته شد، میکروفون گوشی بدون هیچ علامتی روشن می شود.

8-شنود به هنگام برقراری ارتباط:

هر زمان صاحب گوشی اقدام به شماره گیری کرد این ارتباط به طور همزمان به شماره از پیش تعیین شده ای که در گوشی برنامه ریزی شده است ارسال و به اشتراک گذاشته می شود.

9-شنود به روش بهره گیری از کپی سیم کارت مشترکین:

با استفاده موازی از کپی سیم کارت مشترکین می توان مکالمات را شنود کرد.

10- عملیات نفوذ با استفاده از اینترنت مخصوص گوشی های نسل سوم:

هنگام برقراری ارتباط با اینترنت عملیات نفوذ در گوشی برای جاسوس میسر می شود.

11-شنود از طریق کانال های کنترل

12-شنود از طریق مرکز نگهداری و عملیات(OMC)

13- شنود از طریق فرستنده های جاسازی شده در داخل تلفن همراه

14-سوء استفاده های احتمالی از تلفن همراه: مثلا با استفاده از شماره همراه فردی به فرد دیگری تلفن زدن یعنی شماره تلفن او نشان داده شود.

15-ردیابی محل و موقعیت فرد:

غیر از شماره تلفن ها ، شماره سریال گوشی های همراه نیز در شبکه ثبت میشوند. از همین طریق است که محل و موقعیت گوشی های دزدی را شناسایی میکنند. حتی وقتی سیم کارت ناشناسی در آن باشد. همین روش در ردیابی های جاسوسی مورد استفاده قرار میگیرد.

بطور خلاصه: *تلفن همراه چه از طریق سیم کارت و چه از طریق گوشی ابزار بسیار سودمندی برای شنود، جاسوسی ، جمع آوری اطلاعات داخل تلفن و ردیابی مکان و موقعیت فرد است. حتی اگر خاموش باشد.*

توصیه هایی برای مقابله با شنود تلفن همراه :

1. پیشگیری از ورود تلفن همراه به اماکن مهم و جلسات . باتری و سیم کارت موبایل خود را خارج کرده و فضای کاری را عاری از دستگاه تلفن همراه نمایید .
2. کنترل منظم و دوره ای مکالمات وارده به گوشی و تماس های گرفته شده از طریق گوشی
3. کنترل منظم و دوره ای مکالمات انجام شده توسط گوشی، از طریق فهرست مکالماتی شرکت مخابراتی سرویس دهنده
4. چک کردن دائم تماسهای دریافتی و تماسهای گرفته شده در گوشی
5. انجام اختلالات عمدی بوسیله دستگاههای الکترونیکی مثل گذاشتن گوشی کنار سیستم های صوتی و تصویری روشن (البته ممکن است با دستگاه های پیشرفته صداهای مورد نظر فیلتر شوند)
6. استفاده از دستگاه های آشکار ساز های امواج در سالن یا اتاق جلسات مورد نظر به منظور کنترل انتشارات الکترو مغناطیسی
7. حتی الامکان شماره هایی که پیامک های گروهی ارسال می نماید را حذف نمایید .
8. پیامک هایی که از افراد ناشناس می رسد و دارای حجمی بیش از یک اس ام اس است را باز نکنید .
9. بلوتوث دستگاه موبایل خود را در مواقع غیر ضروری ، در حالت Off قرار دهید .
10. اطلاعات شخصی و حساس مانند رمز عبور سامانه بانکی ، شماره حساب و ... را در دستگاه تلفن همراه خود ذخیره ننمایید.
11. در بازه های زمانی کوتاه ، دستگاه تلفن همراه خود را Format نمایید .
12. از استفاده کردن واژهای حساسیت برانگیز در گوشی های تلفن همراه خودداری کنید.

13. نسبت به سریع خالی شدن باطری و یا تلاش بیش از حد دستگاه برای یافتن شبکه(آنتن) حساس باشید زیرا یکی از علایم شنود همین موضوع می باشد.
14. یکی دیگر از راههای احتمالی متوجه شدن شنود، شنیدن پارازیت هنگام نزدیک شدن گوشی به بعضی از دستگاههای صوتی والکترونیکی مانند رادیو می باشد.
15. هر گاه آدرس سرویس دهنده موبایل دچار اختلال شود مجددا باید به این موضوع شک کنیم به طور مثال وقتی IR-TC روی صفحه موبایل تبدیل به IRTC می شود.
16. استفاده از خطوط تلفن ناشناس برای تماسهایی که اصلا نباید شنود شوند.
- مثلا یک سیم کارت اعتباری یا دائمی با نامی غیر از نام خود و گوشی تلفن دست اول
- توصیه مهم تر اینکه موضوعات بسیار خصوصی و حساس را (از ارقام پیشنهادی مناقصه های مالی کلان تا اعتقادات سیاسی حساسیت برانگیز) اصلا پشت تلفن بازگو نکنید.
17. ضد ردیاب: عدم حمل تلفن و یا خارج کردن سیم کارت و باطری از گوشی از مبدا.
18. عدم خرید گوشی های دست دوم یا سیم کارتهای دست دوم

آشنایی با برخی شرکت ها و گوشی های جاسوسی:

امروزه یکی از تجارت های پرسود برای شرکت های سازنده تلفن های همراه ، فروش دستگاه های فعال کننده میکروفون های تلفن های همراه و امکانات شنود این میکروفون های فعال شده می باشد.

از جمله این شرکتها:

شرکت ایتالیایی endoacostica : این شرکت با بهره گیری از فنون خاص دو وضعیت عادی و جاسوسی(روش 5) را برای گوشی های نوکیا مدلهای 2100 و 3310 و 3330 و 3250 و 3390 و 6100 و 6500 و 6610 و 7250 و 8210 و 8250 و 8290 و 8310 و 8850 و گوشی های زیمنس مدلهای c55 و s55 و m50 تعبیه نموده است.

شرکت آلمانی sim: این شرکت اقدام به طراحی گوشی هایی تحت عنوان SIM-A-85 نموده که با روش 3 شنود انجام می دهند.

شرکت آلمانی IBH: اقدام به جاسازی فرستنده های مینیاتوری در داخل گوشی های تلفن همراه Panasonic نموده است.

شرکت فرانسوی cofrexport: با تعبیه حفره های نرم افزاری بر روی گوشیهای ericsson آن را برای اقدامات جاسوسی مهیا نموده و آن را تحت عنوان cof1107 معرفی نموده است.

فصل سوم:

تعقیب و ضد تعقیب

" اصلا من نمی دانم بازجوها از کجا فهمیده بودند که من روزهای جمعه در ساعت 11 صبح می رفتم کوه و در ساعت 7 بعد از ظهر همان روز با دوستانم در پارک قلمستان دیدار می کردم. به این نتیجه رسیدم که همه ی رفت و آمدها و تماس هایم زیر نظر بازجوها بوده است. برای بازجوها مهم بود که بدانند رابطه ی من با دختری که همراه برادرش هم پای من از کوه بالا می آمدند چه می توانست باشد؟ می پرسیدند با آن دختر کجا آشنا شده بودم؟ چی چیز باعث این آشنایی شده بود؟ "(کیانوش سنجری)

در این نوشتار سعی بر این داریم تا اطلاعاتی در ارتباط با شیوه های مختلف تعقیب و راههای مقابله با آن که توسط اشرار امنیتی انجام می شود ارائه دهیم چون همانطور که می دانید و می دانیم مقدمه هر دستگیری ، تعقیب توسط عوامل امنیتی به نیات مختلف می باشد که بعضی از آنها عبارتند ازشناسایی محل زندگی ، شناسایی محل های رفت وآمد ، شناسایی دوستانی که فرد با آنها رفت و آمد دارد ، جمع آوری اطلاعاتی از روابط و عادات رفتاری وی و حتی بستگانش. به قول یکی از آزاد شدگان «علاوه بر اطلاعات، از او تحلیل هم دارند». یعنی می توانند رفتارش را در قبال یک مسئله خاص پیش بینی کنند. به چند مصداق زیر توجه کنید:

"از تکیه کلامی استفاده می کرد که وقتی به دوستانم زنگ می زنم ازش استفاده می کنم و به خودش اجازه می داد راجع به سبک زندگی من اظهار نظر کنه....آره من دختری هستم که همه زندگی ام شده کارم و نه تفریحی و نه دوست پسری !!!! (محبوبه حسین زاده)

"گوشی را از او می گیرم و به پدرم می گویم برای بازداشت من آمده اند و حالا هم می خواهند خانه را تفتیش کنند. می گویند به پدرتان اینطوری نگویید، هول می کنند و برای سلامت قلبشان خوب نیست. در دل می گویم از بیماری بابای من هم که خوب اطلاع دارید!"(فرناز سیفی)

"او من را به خوبی می شناخت. می دانست که با روحانیت هیچ ارتباطی نداشته ام و حتی به من اطلاع داد که برای دوستانم غیر منتظره بوده که من در تحصن یک روحانی و هوادارانش بازداشت شده بودم. معلوم بود که مکالمه های تلفنی دوستانم را شنیده بودند."(کیانوش سنجری)

معمولا دو هدف عمده از جمع آوری اطلاعات ریز و درشت از زندگی فرد مد نظر اشرار امنیتی است:

- سوء استفاده و پاپوش سازی برای قطور کردن پرونده وی
- تضعیف و شکستن روحیه فرد.
- البته در مورد خواص و مسئولین مملکتی با هدف اخاذی یا باج خواهی یا حق السکوت در موارد گوناگون صورت میگیرد.

بنابراین آگاهی از فنون ضد تعقیب (چه کار کنیم که تعقیب نشویم و راههای خارج شدن از آن) بسیار مهم است . در ادامه توصیه هایی در این زمینه شده است که به کار بستن آنها می تواند بسیار راهگشا باشد.

شیوه های اطلاع و پیشگیری از تعقیب شدن:

1. هنگام ترک محل ، هوشیاری و مراقب بودن نسبت به افرادی که در اطراف شما هستند. خصوصا ماشینهای پارک شده در دیدرس منزل یا مکان مورد نظر.
2. گاهی تعقیب کنندگان در هنگام تحت نظر داشتن مکان، دو ماشین را طوری پشت سر هم پارک میکنند که ماشین دوم نزدیکتر به جدول کنار خیابان و تورفته تر از ماشین جلویی است در نتیجه از فاصله چند متری افراد در داخل ماشین عقبی دیده نمیشوند. اینطور بنظر میرسد که در کوچه هیچ فردی داخل ماشین نیست. بنابراین توصیه میشود داخل ماشینها را از فاصله نزدیک نگاه کنید.
3. مسیرهای خود را تغییر دهید. و همیشه از یک مسیر تکراری و مکانهای تکراری (یک کافی نت همیشگی یا ایستگاه مترو یا تاکسی مشخص و ثابت) استفاده نکنید.
4. همیشه در یک ساعت مشخص از محل کار یا منزل خارج نشوید.
5. همیشه از یک کافی نت استفاده نکنید.
6. هنگامیکه در مسیری در حال رفتن هستید گاه به گاه توقف و به چهره افرادی که در پشت سرتان هستند توجه کنید.
7. قدم زدن در یک پارک یا خیابان دور افتاده و خلوت یک تعقیب را کاملا مشخص می کند افراد یا فردی شما را به صورت نامحسوس همراهی میکنند یا نه.
8. داخل شدن به ساختمانی و بلافاصله خارج شدن از آن راه دیگری برای تشخیص تعقیب است.
9. سوار اتوبوس یا مترو شوید و مشاهده کنید که آیا شخصی با شما سوار و هم زمان پیاده می شود یا خیر.
10. سرعت قدم زدن را تغییر دهید ، توقف کرده و وقت گذرانی نمائید ، مسیر خود را ناگهانی عوض کنید.
11. سوار شدن به آسانسور و پله برقی.
12. گاهی تکه کاغذی یا شئی به زمین بیاندازید تا ببینید کسی آن را برمیدارد یا نه؟
13. از مکانهای خلوط برای مسیر خود استفاده کنید که تعقیب کننده ها در شلوغی خود را استتار نکنند.
14. از ماموران اداره برق و .... که زمان غیر معمولی را نزدیک خانه یا محل کار شما میگذرانند، بی دقت نگذرید.

فرار و گریز از تعقیب با پای پیاده:

1. سوار یک وسیله نقلیه عمومی شده در نزدیک درب توقف نموده به محض حرکت وسیله از آن به پایین بپرید.
2. هنگام حرکت یک وسیله نقلیه سوار بر آن شوید (عکس حالت اول).
3. هنگام حرکت به سمت درب وسیله نقلیه با عجله حرکت کرده اما پیاده نشوید ، تعقیب کننده خطا کرده و پیاده می شود.
4. سوار آخرین تاکسی ایستاده در ایستگاه شوید.

اگر شما پیاده و تعقیب کنندگانتان سوار ماشین هستند:

1. در خیابان یکطرفه در جهت خلاف حرکت کنید.
2. در اتوبان و یا بزرگراه با دیدن پل عابر پیاده از پل به سوی دیگر اتوبان بروید و با گرفتن ماشین از انجا دور شوید.
3. در خیابان معمولی خود را در جمعیت زیاد گم کنید.
4. از ساختمانها و مکانهایی که دارای دربهای خروجی متعددی هستند استفاده کنید. مثلا به فروشگاههای بزرگ مانند شهروند وارد شده و از درب دیگر آن خارج شوید.

فرار از تعقیب با اتومبیل خودتان :

1. ساده ترین راه برای متوجه شدن از تعقیب این است که مستقیما به طرف مقصد نروید.
2. چرخش در یک زاویه قائمه کمک می کند تا تعقیب کننده مشخص شود.
3. اگر شخص دیگری در اتومبیل تان باشد ، کمک شایانی به شما می کند.
4. با تغییر سرعت می توانید متوجه شوید کسی شما را تعقیب می کند یا خیر ، با کم کردن سرعت اتومبیل های تعقیب کننده از شما سبقت نمی گیرند.
5. اگربا سرعت بسیار کم حرکت کنید، متوجه می شوید کسی شما را تعقیب می کند یا خیر.
6. به گوشه ای رفته و پارک کنید دقت کنید کسی با شما پارک می کند یا خیر.
7. در صورت تعقیب و گریز با ماشین میتوانید با بیرون ریختن کاغذ پاره هایی که مهم هم نیست، حواس تعقیب کننده ها را پرت کنید اما همیشه ممکن است کاغذ هایی که شما بیرون ریختید برایشان مهم نباشد و به تعقیب تان ادامه بدهند.
8. در شب با چراغ های خاموش پارک کرده و در صندلی فرو روید این عمل باعث می شود تا تعقیب کننده ها شما را گم کنند.
9. با سرعت زیاد رانندگی کرده و ناگهان اتومبیل خود را در گوشه ای پارک نمائید. (باعث می شود تعقیب کننده دچار اشتباه شود)
10. به یک خیابان ورود ممنوع وارد شوید. این روش مطمئنی است که متوجه شوید کسی در تعقیب شما است یا خیر.

11. یک پیچ و گردش ناگهانی راه دیگری برای شناسایی تعقیب کننده است . هر اتومبیلی که به دنبال شما دور بزند از داخل آئینه قابل رویت خواهد بود.
12. سرعت را قبل از رسیدن به چهارراه های که چراغ راهنمایی دارند طوری تنظیم کنید که هنگامیکه چراغ قرمز می شود به آن رسیده و از آن عبور کنید.
13. ورود به داخل یک خیابان بن بست شیوه دیگری برای شناسایی تعقیب کننده است.
14. بررسی کنید آیا اتومبیل تان از نظر ظاهری دچار تغییر شده است یا خیر مثلا چراغ خطر شکسته شده است یا خیر زیرا یکی از راه ها برای متمایز کردن اتومبیل سوژه از بقیه اتومبیل ها این کار است.
15. احتمال دارد تعقیب کننده با نصب وسایل الکترونیکی بر روی اتومبیل یا با استفاده از جی پی اس، شما را از فاصله دور بتواند تعقیب کند. اگر مطمئن شوید که این کار انجام شده وسیله الکترونیکی را پیدا کرده و آنرا به اتومبیل دیگری وصل کنید (معمولا آهنربایی است). یا چیزی مثل تلفن همراه را که جی پی اس دارد را خاموش و سیم کارت و باطری آن را کاملا از هم جدا کنید.
16. راه دیگر تعویض اتومبیل در زمانهایی است که نمیخواهید تعقیب شوید و یا مبادله ماشینتان با ماشینی همان مدل و همان رنگ.
17. تغییر مسیر ناگهانی بدون زدن راهنمای اتومبیل .
18. انداختن اشیایی از داخل ماشین به بیرون جهت انحراف توجه تعقیب کنندگان
19. از اتومبیلی استفاده کنید که جلب توجه نکند مثلا رنگش معمولی باشد یا اینکه وسیله ای روی آن نباشد که بتواند آنرا به راحتی از اتومبیل های دیگر تمایز داد.
20. نقشه شهرتان را بشناسید تا به راحتی بتوانید از تعقیب عبور کنید.

<u>مواردی را که تعقیب کنندگان رعایت می کنند و ما باید آنها را بدانیم :</u>

1. آنها ظاهری طبیعی و معمولی دارند.
2. معمولا طوری رفتارمی کنند که برای سوژه جلب توجه نمی کنند.
3. هنگام سوار و پیاده شدن در وسایل نقلیه عمومی با سوژه هماهنگ هستند.
4. آنها مراقب مکانهایی که دارای چند راه ورود و خروج می باشدهستند.
5. بعد از اینکه سوژه آنها را شناسایی کرد ، معمولا به طرق مختلف تغییر قیافه می دهند.
6. معمولا در تعقیب پیاده از راه دور طوری که جلب توجه نکنند کار خود را انجام می دهد.
7. آنها گاهی اوقات مبادرت به عکس و فیلم برداری از سوژه می نمایند(در تماس با دیگران این احتمال را بدهید که از شما تصویر برداری میشود.)
8. گاهی اوقات آنها در پوشش ماموران شهرداری (رفتگر) و غیره ظاهر می شوند.

9. آنها گاهی اوقات برای کسب و جمع آوری اطلاعات از سوژه های خود از ماشینهای بزرک مانند مینی بوس که دارای پرده است استفاده می کنند و از داخل آن مبادرت به فیلم برداری از سوژه می نمایند.

نکات عمومی

1. ارتباطات مهم تان با وسایل ارتباطی که همیشه از انها استفاده می کردید نباشد مثلا از تلفنی که به طور معمول از آن استفاده می کنیدو یا آدرس ایمیلی که همه از آن اطلاع دارند و یا موارد مشابه.
2. رفتار و گفتارتان عادی باشد مثلا از بعضی کلمات حساسیت بر انگیز در مکالمات تلفنی استفاده نکنید.
3. نیازی نیست از برنامه ها و اطلاعاتی که مختص شماست دیگران مطلع باشند حتی اقوام و دوستان نزدیک.
4. برخوردتان با دیگران عادی باشد و مانند یک شهروند معمولی عمل کنید.
5. هنگام شرکت در اجتماعات و مکانهایی که اشخاص شناسایی می شوند تغییر قیافه بدهید یا از ماسک و شال گردن استفاده کنید.
6. تدبیری کنید که اطلاعات و اشیا مهم تان به راحتی قابل از بین رفتن باشد به طور مثال کلیه اطلاعات لازم و مهم را در یک کول دیسک یا ترجیحا میکرو اس دی(micro sd) باشد که سریعا قابل از بین بردن باشد.
7. هنگام رفتن به مکانها ی حساس یا دور شدن از حوزه تعقیب، موبایل معمولی خود را به هیچ عنوان همراه نبرید، زیرا یکی از مهمترین راههای ردیابی شما می باشد.ترجیحا هیچگونه تلفنی به همراه نداشته باشید. به ایمیل و فیس بوک و ... خود سر نزنید. به تلفن هیچ یک از دوستان و آشنایان از آن مکان زنگ نزنید.

...

منابع:

- وبلاگ دانشجویان مهندسی فناوری اطلاعات http://bsu.blogfa.com/
- سایت دویچه وله مصاحبه با محمود تجلی‌مهر، کارشناس مخابرات
- h p://thegodtha ailed.wordpress.com/2009/07/06/an-espionage-solutions-for-us
- h p://elminews.blogspot.com/2009/07/blog-post_4566.html
- http://egov-security.ir/index.php?op on=com_content&task=view&id=34&Itemid=1
- http://iranictnews.ir/H .htm