**بسم الله الرحمن الرحیم**

**شیوه هاي نوین جاسوسی**

**مقدمه:**

انقلاب ديجيتالي و پديده هاي نوظهوري چون، اينترنت، **وب ها و وبلاگ ها** گرچه با پيشفرض سياسي و جاسوسي طراحي و توسعه نيافت اما مانند اكثر اختراعات بشري ، بستري شد براي سوء استفاده ي سياسيون و دستگاههاي اطلاعاتي غرب از شهروندان خود و ديگركشورهاي به مرور با عميق تر شدن اين به اصطلاح انقلاب و ايجاد و شبكه هاي اجتماعي شكل گرفت و سامان يافت به مرور سازمانهاي اطلاعاتي غرب درك كردند كه اين شبكه هاي اجتماعي بالقوه ميتوانند بستري بسيار مناسب براي كسب اطلاعات علني و يا احياناً غيرعلني باشند.

ويژگي خاصي كه اين شبكه ها براي سازمانهاي اطلاعاتي داشتند آن بود که مي توانستند اين بار برخلاف گذشته آنها نهايتاً اطلاعات علني را مي بايد از طريق رسانه ها بدست مي آورند اين بار به صورت مستقيم با مردم در كشور هدف ارتباط داشته باشند تا نظراتشان را بخصوص در مورد يك خبر خاص و مشخص را بدانند. اين امري بود كه پيش از اين به واسطه ي وبلاگها هم امكان تحقق داشت اما ضعف وبلاگها در اين مورد عدم دسته بندي و تفكيك اطلاعات بود كه كار بررسي و تحليل خبر را وقت گير وپرهزينه مي نمود گرچه ابتدا امر **تويتر** مي توانست به عنوان يك **ميكروبلاگر** به كمك آن بيايد.اما در نهايت شبكه هاي اجتماعي عملاً توانسته بودند اين ايرادبزرگ وبلاگها را نيز برطرف كنند.

در واقع آنچه به خصوص در اين شبكه هاي اجتماعي اتفاق مي افتد، بكارگيري و تخليه اطلاعاتي مخاطب است بدون اينكه وي كوچكترين آگاهي از اين امر داشته باشد و طرف اصلي را در اين شبكه ها بشناسد.

شبكه هاي اجتماعي حافظ منافع سازمانهاي جاسوسي غربي در جريان حوادث پس از فتنه سال1388 ، خبري در رسانه هاي خارجي منتشر شد مبني بر اين كه وزارت خارجه آمريكا از گردانندگان شبكه هاي اجتماعي نظير **فيس بوك و تويتر** خواسته است تا فرآيندروزآمدسازي فصلي خود را به تاخير بيندازد تا معترضين با استفاده ازاين شبكه ها با يكديگر ارتباط برقرار كنند.اما سوالي كه در اينجا مطرح ميشود اينست كه آيا واقعاً علت اصلي درخواست دولت آمريكا از اين شبكه ها همين مورد بوده؟

براي پاسخ به اين سوال پيش از هر چيز بايد به طرز تفكر و فلسفه روسا و اساساً سيستم اطلاعاتي غرب پي برد.براي اين كار ابتدا بايد نوع اطلاعات مورد نياز يك دستگاه اطلاعاتي را بشناشيم اطلاعات موردنظر يك دستگاه اطلاعاتي از يك نظر به دو نوع تقسيم ميشوند.

**1)اطلاعات علني**

**2) اطلاعات غيرعلني** : براساس گفته ي متخصصين طراز بالاي سيا 95 درصد اطلاعات موردنياز از اطلاعات علني تامين ميگردد و تنها 5 درصد آژانس اطلاعات مركزي »اطلاعات طبقه بندي شده است.

**اطلاعات علني**، اطلاعاتي است كه مطبوعات، رسانه ها و مردم كوچه بازار آن را در اختيار دارند و **اطلاعات غيرعلني** يا طبقه بندي شده همانند يك سند طبقه بندي شده نظامي مي باشد كه براي به دست آوردن سازمان هاي اطلاعاتي مجبور به اجيركردن نيرو و هزينه هاي زياد مي باشند كه با توجه به نوع سندي كه توسط اين مزدور ميتواند كشف شود و خطرات احتمالي لو رفتن اين جاسوس، كسب چنين اطلاعاتي داراي ريسك بالايي مي باشد .

سازمانهاي اطلاعاتي معمولاً براي بدست آوردن اطلاعات خارجي از دو روش كلي ولي با قواعد يكسان استفاده ميكنند. اين روشها عبارتند از:

**1 ) از طريق پايگاه برونمرزي)خارج از كشور هدف)**

**2) از طريق پايگاه در كشور هدف كه البته بايد حتماً داراي پوشش باشد نظير سفارتخانه و ساير پوششهاي ديگر.**

براساس همين مطالب مي توان بسياري از حركات و كردارسازمان هاي اطلاعات جهان را در قبال كشورمان تحليل كرد ضمن اين كه بايد در نظر داشت كه بارها خود مسولين اطلاعاتي و سياسي اين كشورها خصوصا آمريكا تاكيد داشته اند كه بزرگترين نقطه ي ضعف آنها در قبال ايران نداشتن اطلاعات از داخل ايران است.

آن زمان كه ايالات متحده سعي مي كند با ايجاد پايگاههايي دركشورهاي اطراف ايران به كسب اطلاعات ازداخل ايران بپردازد درواقع به سبك پايگاههاي برون مرزي مشغول كسب خبر است و چه آن زمان كه دولت آمريكا فشاذ مي آورد كه در ايران كنسولگري داشته باشد در واقع به دنبال كسب خبر با استفاده از تكنيك ايجاد پايگاه در كشورهدف است.

در سالهاي پس از پيروزي انقلاب اسلامي آمريكا به لطايف الحيل و با استفاده از روشهايي كه گفته شد و با صرف هزينه هاي فراوان سعي كرده كه ضعف اطلاعات خود را در قبال ايران برطرف كند.

اما هر چه بيشتر هزينه كرده، كمتر نتيجه گرفته است: شايد دو دليل اصلي كه باعث شده است تا اينگونه اقدامات كمتر نتيجه داده عبارت باشند از:

1. **احساسات شديد ملي گرايانه ايرانيان**

**2)هوش اجتماعي بالاي ايرانيان** كه باعث ميشود به راحتي اقسام و انواع پوششها را درك كرده و از اينگونه سازمانها فاصله بگيرند.اين دلايل باعث شده است كه همواره عده هاي خاص كه داراي عقايد مشخص سياسي - مذهبي هستند با اينگونه سازمانها ارتباط برقرار كنند كه خود همين باعث مي شود نتايج اطلاعات دريافتي از اينگونه افراد با واقعيت جامعه تفاوت زيادي داشته باشد.

در واقع ضعف عظيم سازمانهاي اطلاعاتي غرب در قبال ايران آن است كه اين كشورها از عقايد عامه مردم و طرز تفكرشان، آداب، سننشان اطلاعات درستي ندارند و آن اطلاعاتي را هم كه در اختيار دارند يا دريافت ميكنند را معمولاً به واسطه ي افراد با پيش زمينه هاي مشخص كسب ميكنند.

آيا شبكه هاي اجتماعي قابل نظارت هستند؟همه كارشناسان و آحاد مردم بر اين باورند كه پيشگيري بهتر ازدرمان است.

ما تنها سلاحي كه مي توانيم در برابر اين شبكه ها داشته باشيم**،فرهنگ سازي** است. عليرغم ميلياردها ريال هزينه جهت فيلترسازي سايتها، مشاهده مي گردد كه فيلتر تاثيري ندارد چرا كه شركت هايي وجود دارند كه در خارج از كشور به منظور مبارزه با اين روند با مستمسك قراردادن آزادي بيان نسبت به فروش انواع فيلتر شكن ها، ساكسها، وي پي انها و ... در جامعه ما علاوه بر كسب درآمدها كلان، كليه هزينه هاي صورت گرفته از سوي دولت جهت اعمال فيلتر را تباه مي سازند.

لذا مي بايست همزمان با فيلترسازي،در راستاي اعتلاي فرهنگ استفاده از اينترنت در سطح جامعه گام هاي مؤثري برداشته شود تا بتوان با اين پديده جديد مقابله نمود.

**فيلترينگ فيسبوك،وي چت،اينستاگرام** و باقي شبكه هاي اجتماعي سودمند نيست زيرا هر روز بر تعداد اينگونه شبكه ها افزوده ميشود. بسياري از كارشناسان معتقدند كه فناوريهاي جديد مانند شمشيردو لبهاي هستند كه از سويي نعمت تلقي مي شوند و از سوي ديگر نقمت مشكل آنجاست كه پيش از آنكه فرهنگ استفاده از اين فناوريها و شيوه صحيح بهره گيري از آنها در ميان مردم فراگير گردد، به سرعت جذابيت آنها چشم مردم و به خصوص جوانان را پر ميكند؛به گونه اي كه روز به روز شاهد آسيبهاي اجتماعي جبران ناپذير ناشي از استفاده نامناسب از اين فناوريها مخصوصا شبكه هاي اجتماعي نو پديد هستيم. از رقابت براي خودنمايي در اين شبكه ها تا پخش شدن عكسهاي خصوصي و گسترش فساد و عادي شدن آن براي افراد به ويژه جوانان!

آشنايي با جاسوسان پنهان عرصه ديجيتال با فراگير شدن رسانه ها و شبكه هاي اجتماعي نظير "فيسبوك" و "توئيتر"، نرم افزارهاي اين سرويسها نيز به تلفنهاي هوشمند سرازير شده اند.

افراد با درج اطلاعات، افكار و عقايد و برنامه هاي روزانه خوداز طريق شبكه هاي اجتماعي، به دستگاه جاسوسي آمريكا امكان پايش آني تمامي جنبه هاي زندگي شخصي افراد را مي دهند. از موقعيت مكاني گرفته تا مكالمات و ارتباطات و افكار و عقايد و فعاليتهايي كه قرار است در آن لحظه انجام دهند.

از اين رو **تلفنهاي هوشمند** به بزرگترين دام شبكه جاسوسي آمريكا تبديل شده اند كه به سادگي همگان را به كام خود فرو ميكشند.فيسبوك، توئيتر، يوتيوب و ديگر شبكه هاي اجتماعي از ديد سازمان هاي اطلاعاتي به عنوان كانالهاي شديدا باارزشي براي كسب اطلاعات به حساب ميآيند.

ما يافته هاي خود را بر اساس سه مطالعه موردي اخير بنا مي كنيم كه به عقيده ما عملكرد اطلاعاتي شبكه هاي اجتماعي را نشان ميدهند.البته شبكه هاي اجتماعي تنها يك ابزار جمع آوري اطلاعات نيست و سازمانهاي جاسوسي از شبكه هاي اجتماعي براي اهداف ديگري نيز سوء استفاده ميكنند.و رسوايي جاسوسي كاخ سفيد از « **ادوارد اسنودن » ماجراي شهروندان كشورهاي مختلف جهان**، در گذشته آنقدر سروصدا كرده كه تقريبا همه كاربران اينترنت چيزي درباره آن شنيدهاند و يا مطلبي درباره آن خوانده اند؛

 البته يقينا بيشتر اين مطالب درباره درگيريهاي آمريكا با روسيه بر سر تحويل دادن اسنودن بوده و نه اصل ماجرا، كه مسبب اصلي بالا گرفتن اين ماجرا شد.از هاوايي به هنگ كنگ، « ادوارد اسنودن » ماجرا از آنجا آغاز شد كه جايي كه در آن براي يكي از تاسيسات آژانس امنيت ملي امريكا كار مي كرد، گريخت؛ البته وي اسنادي درباره برنامه هاي نظارت اينترنتي و تلفني فوق محرمانه امريكا را نيز در دست داشت. پس از آن، اسنودن در يك ويدئو كه گاردين آن را منتشر كرد، به نقش خود در افشاي اين اطلاعات اشاره كرد و در اين مصاحبه» افزود كه تنها انگيزه وي آن است كه افكار عمومي را از آنچه به نام آنان و يا بر ضد آنان انجام مي شود، آگاه كند و حاضر است زندگي راحت خود را فدا كند؛ چرا كه نمي تواند با وجدان آسوده به دولت امريكا اجازه دهد با اين ساز و كار جاسوسي بزرگ كه مخفيانه سرگرم ساخت آن است، حريم خصوصي، آزادي اينترنتي و آزاديهاي اساسي مردم در سراسر دنيا را نابود كند.اسنودن ابتدا به هنگ هنگ رفته و پس از اطلاع منابع اطلاعاتي چين از اين مكان، سر از روسيه، به عنوان رقيب چند ده ساله اطلاعاتي آمريكا سر درآورده است. پس از اين رويداد بود كه درگيريهاي لفظي ميان **كرملين و كاخ سفيد** بر سر بازپس دادن او بالا گرفت و به تيترنخست بسياري از رسانه هاي جهان تبديل شد.

اما اصل ماجرا چه بود؟ درگيري مسكو و واشنگتن، حاشيه اين رسوايي بزرگ است. اصل ماجرا، جاسوسي رسمي، قانوني و نظام مند دولت آمريكا از كاربران اينترنت است كه به طور رسمي صورت مي گيرد و اكنون بخشي از آن افشا شده است.

روزنامه گاردين حكم فوق محرمانه دادگاهي در امريكا را فاش كردكه به آژانس امنيت ملي اين كشور اجازه مي دهد ، ورايزون » امريكايي كه مشتري شركت ارتباطي اطلاعاتي هستند « روزانه درباره ميليونها نفر اطلاعات جمع آوري كند. طبق اين حكم، ورايزون بايد به صورت همچون شماره تلفن، محل، زمان و مدت تماس تمامي مكالمات تلفني انجام شده در سيستمهاي خود چه در داخل امريكا و چه خارج از آن را در اختيار آژانس امنيت ملي قرار دهد.

در همان روز با اشاره به دسترسي مستقيم آژانس « واشنگتن پست »امنيت ملي امريكا به سرورهاي شركتهاي اينترنتي اعلام كرد منبع اين روزنامه كه مامور اطلاعاتي يكي از شركتهاي حمل و نقل است ازتوانمنديهاي سيستم هاي مورد استفاده آژانس جاسوسي عالي رتبه امريكا دراين زمينه وحشت كرد.دولت اوبامادرحال حاضر به علت شنود مخفيانه مكالمات تلفني خبرنگاران آسوشيتدپرس وهمچنين نظارت برايميل ها و مكالمات تلفني خبرنگاران شبكه خبري فاكس نيوزبه شدت موردانتقاد قرارگرفته است ؛ انتقاداتي كه اكنون در برابر اين رسوايي عظيم جاسوسي،كم اهميت به نظر ميرسند.

سالهاست كه كارشناسان ارتباطات و فناوري اطلاعات از جاسوسي عظيم شبكه هاي اجتماعي از كاربران اينترنت در سراسر جهان سخن ميگويند؛ يك جاسوسي شيك و تميز كه از خود شما به عنوان عامل اطلاعاتي استفاده ميشود.

اسناد جديدي كه اسنودن منتشر كرده، مربوط به بخش عمليات منبع ويژه آژانس امنيت ملي آمريكا است. اين بخش مسئول تمام برنامه هايي است كه با هدف نظارت بر ارتباطات آمريكاييها طراحي شده است.اين اسناد نشان ميدهد آژانس امنيت ملي آمريكا از همان زمان كه در ماه جولاي سال گذشته راه « آوتلوك » سرويس چت رمزبندي شده افتاد، نسبت به آن نگراني پيدا كرده است. در عرض پنج ماه بعد از آن،مايكروسافت و اف بي آي توانستند براي رمزگشايي از اين اطلاعات دست يابند و آن را در اختيار آژانس امنيت ملي قرار دادند.

در يكي از نامه ها آمده است: مايكروسافت و اف بي آي برنامه جاسوسي طراحي براي حل اين موضوع طراحي كرده اند. اين برنامه با موفقيت تست و عملياتي شده است. دو ماه بعد از اين بود كه مايكروسافت رسما سامانه **. Outlook**. **com** راه اندازي كرد همچنين، آژانس امنيت ملي آمريكا در طول سال هاي گذشته تلاش زيادي كرده است تا با همكاري مايكروسافت بتواند توانايي خود را افزايش دهد. اين آژانس بعد از « **اسكايپ** اطلاعات منتقل شده درآنكه اسكايپ به مايكروسافت واگذار شد، اين توان را پيدا كرد كه حجم دادهاي ذخيره شده از ارتباطات با اسكايپ را سه برابر كند. اين اقدام كه با همكاري مايكروسافت انجام گرفت، با روش حذف تصاويرويدئويي و نگهداري بخش صوتي ممكن شد. در خبري كه يكي از سايتهاي اينترنتي اعلام كرده، مشخص شده كه گوگل قصد دارد تا در منابع جستجوي كاربران گوگل، از محتواي جيميل آنها هم استفاده كند؛ يعني رباتهاي گوگل ابتدا متن تمام ايميلهاي شخصي شما را كه ممكن است حاوي نامه محرمانه هاي شما ، درخواست كار به يك شركت و يا حتي يك تبريك سال نو به دوستتان در اروپا باشد را مي خوانند و سپس با توجه به كليد واژ ه هاي استفاده شده در اين ايميلها، تبليغات مرتبط با تمايلات و سليقه شخصي شما را در جيميل به نمايش ميگذارد.

البته شايد در نگاه اول اين مساله خوشايند به نظر برسد؛ چرا كه همه كاربران اينترنتي از تبليغات اسپم خسته شده اند و تغيير تبليغات متناسب با ذائقه آنها قطعاً خبر خوشحال كننده اي خواهد بود اما واقعا چه كسي است كه علاقه داشته باشد تا تك تك نامه هاي شخصي اش توسط گوگل خوانده و احيانا ذخيره شود؟ تصور اينكه شما يك نامه حاوي اطلاعات محرمانه براي رئيس خود مي نويسيد ولي پيش از آنكه به دست او برسد، محتواي آن در مانيتور يكي از كارمندان گوگل دركاليفرنيا به نمايش در بيايد، واقعا وحشتناك است!

شبكه هاي اجتماعي ؛ **منافذ جاسوسي موساد** در سراسر دنيا ارتباط رايانه هاي شخصي با اينترنت و شبكه هاي اجتماعي در نقاط مختلف جهان، كار دستگاه جاسوسي رژيم صهيونيستي را براي سوء استفاده از افراد و جاسوسي ساده تر كرده است. به گزارش سرويس بين الملل باشگاه خبرنگاران به نقل از شبكه العالم ؛ اين روزها ديگر ضرورتي ندارد كه افسران موساد براي جذب جاسوس تلاش بسياري را انجام دهند، چرا كه آنها از طريق شبكه هاي اجتماعي افراد را ندانسته به منبعي اطلاعاتي تبديل ميكنند.

روزنامه "الحيات" در مطلبي درباره شيوه هاي جديد جاسوسي موساد، نوشت:فيسبوك منبع اطلاعاتي مهمي براي موساد است؛ اين سرويس جاسوسي از طريق فيسبوك از اوضاع فلسطيني ها مطلع ميشود واطلاعات موجود در كامپيوترهاي شخصي افراد را به دست مي آورد .

چگونگي نفوذ موساد به رايانه هاي شخصي : موساد هزاران صفحه در فيسبوك ايجاد ميكند و هر يك از افسران اين سرويس جاسوسي تعدادي از اين صفحات را كنترل ميكنند؛ آنان براساس اطلاعات روزانه اي كه از دوستان فيسبوكي خود جمع آوري مي كنند؛ گزارش هايي روزانه، هفتگي، ماهانه و سالانه را درباره اوضاع فلسطيني ها تهيه مي كنند.

موضوعات اين گزارشها شامل مسائل امنيتي، اقتصادي، معيشتي،سطح فرهنگي جوانان، ارتباط فلسطينيها با دولت و ديدگاه فلسطينيهادرباره مقاومت و شليك موشك و غيره است .افسران موساد براساس اطلاعاتي كه از فيسبوك جمع آوري ميكنند، در گزارش خود به مقامات ارشد اين سرويس جاسوسي طرح اجير كردن تعدادي ازدوستان فيسبوكي خود را پيشنهاد ميكند.

افسران موساد در شرايط جنگي و درگيريهاي مرزي درپي جمع آوري اطلاعاتي درباره محل شليك موشك، تجمع اعضاي گروههاي مقاومت، وضعيت روحي فلسطينيها و ميزان حمايت فلسطينيها از مقاومت هستند كه با جمع آوري اين اطلاعات و بررسي دقيق آن نقشه ها و اهداف خود را آماده ميكنند .

مرحله خطرناك؛ دستيابي موساد به اطلاعات رايانه هاي شخصي براي نفوذ به هر رايانه شخصي وجود 2 عامل مهم است، **اولين است و عامل دوم نصب برنامه جاسوسي در ( IP ) عامل اي پي كامپيوتر؛ بدون اين دو عامل يا يكي از آنها نفوذ به كامپيوتر شخصي امكان ندارد .**

روش دست يابي به آي پي رايانه شخصي از طريق ايميل يافيسبوك :**از طريق ايميل : در صورت ارسال ايميل به افسر موساد، وي از طريق ايميل ارسالي به اي پي رايانه ارسال كننده ايميل پي خواهد برد .از طريق فيسبوك:  افسر موساد در فيسبوك درخواست دوستي براي فردي ميفرستد، وبه محض موافقت آن فرد با اين درخواست دوستي ، فيسبوك پيام وي را از طريق ايميل به افسر موساد ميفرستد؛** ارسال هرگونه ايميل يا اظهار نظر روي صفحه شخصي افسر موساد به معناي مطلع كردن اين جاسوس از آدرس آي پي رايانه شخصي است.موساد چگونه در رايانه هاي شخصي برنامه جاسوسي نصب ميكند**: افسر موساد پس از به دست آوردن آدرس اي پي، براي نصب برنامه جاسوسي روي كامپيوتر شخصي افراد لينك اين برنامه را با عناوين فريبنده مانند دانلود تصوير و موسيقي ارسال ميكند تا فرد مورد نظرروي لينك كليك كند؛ افسر موساد با كليك كردن افراد روي لينك ارسالي وارد كامپيوتر شخصي آنها ميشود؛ از اين به بعد هر چيزي كه روي صفحه كامپيوتر فرد مورد نظر ظاهر يا تايپ شود، مي بيند و ثبت ميكند.**

ترفندهاي تكنولوژيك غرب براي جاسوسي تلفني تلفن هاي همراه داراي نوعي باطري بسيار ريز با عمر دست كم 50 ساله است كه در مواقع حساس و مورد نياز براي كشور ها و سيستم هاي اطلاعاتي ناظر بر ساخت اين گوشي ها اطلاعات ارسال خواهدنمود.شاهد مثال اين قضيه نيز زماني است كه به هر دليل گوشي خودرا گم كرده و از مخابرات تقاضاي يافتنش را داشته باشيد، كه با رعايت جميع شرايط، گوشي شما در صورت خاموش بودن نيز پيدا خواهد شد

**تخليه تلفني چيست**؟موضوعي كه در عين سادگي و كم اهميت جلوه كردنش بسيار مهم و حياتي است و بسيار به امنيت كشور خدشه وارد كرده است.شايد اولين سئوالي كه به ذهن خطور مي كند، اين باشد كه تخليه تلفني به چه معناست؟

**تخليه تلفني در معناي عام** به معناي به دست آوردن اطلاعات ازافراد مختلف جامعه توسط تلفن، به وسيله ي كساني كه به هر دليل عناد با اين مرز و بوم دارند اطلاعاتي كه از نظر ما اهميت چنداني نداردمثل اسم رئيس يا همكار ، همسر يا ارائه آمار هاي خيلي معمولي درحيطه كاري تعريف **تخليه تلفني به صورت كلاسيك** :تخليه تلفني، عبارت استاز تلاشي آگا هانه از طرف دشمن با بهره گيري از غفلت يا فريب عوامل خودي، به منظور كسب اطلاعات و القاي خواسته هاي خود ازطريق برقراري ارتباط تلفني.

**اهداف دشمن از تخليه تلفني** :جمع آوري اطلاعات در خصوص مشكلات داخلي جامعه در راستاي بهره برداري تبليغي - شناسايي مشكلات دستگاههاي اجرايي، جهت بهره برداري تبليغي در راستاي ناكارآمد نشان دادن نظام - كسب اطلاعات، در راستاي دامن زدن به اختلافات جناح هاي سياسي كشور -تلاش آگا هانه براي ايجاد اختلافات مذهبي ، سياسي و قومي در داخل كشور -كسب اطلاعات با هدف ايجاد اخلال در روابط جمهوري اسلامي در مجامع بين المللي اولين سئوالي كه در اين خصوص مطرح است اينكه به نظر شماچند درصد از اطلاعات و اخبار كشور توسط تخليه تلفني به دست دشمنان ايران زمين مي افتد؟پاسخ : نزديك به 80 درصد اطلاعات كشور توسط تخليه تلفني ازتمامي اقشار جامعه به دست دشمنان اين مرز و بوم مي افتد.

سئوال بعدي كه مطرح ميگردد اين كه دشمن در تخليه تلفني به دنبال چيست و چه كساني در معرض تخليه تلفني هستند؟پاسخ : دشمن در تخليه تلفني به دنيال اطلاعاتي است كه از نظر ما ارزش چنداني ندارند، ولي در واقع براي آنها ارزشمند محسوب ميگردد و اطلاعات ما به واقع تكميل كننده پازل اطلاعاتي آنهاست ودشمنان براي اين كار هيچ محدوديت سني اعمال نكردند و از كودكان 6 ساله تا سال خوردگان 90 ساله را مورد تخليه قرار داده اند.

اصولاً تخليه تلفني به دو صورت انجام مي گيرد:

1. **كنترل تلفن همراه افراد با استفاده از وسائل و روشهاي مخصوص، كه بيشتر جنبه ي جاسوسي و اطلاعاتي دارد.**
2. **تماس تلفني با اشخاص و گرفتن مستقيم اطلاعات از آنها**:

طبق تحقيقات سازمان هاي اطلاعاتي كشور هاي مختلف ثابت گرديده است كه تلفن هاي همراه ساخته شده توسط كارخانه هاي مختلف داراي يك حافظه مخفي با ظرفيت بالا جهت ضبط مكالمات و يك وسيله اي شبيه سيم كارت به صورت مخفي جهت ارائه اطلاعات گوشي مورد نظر به كشور هاي سازنده در مواقع خاص است و تلفن هاي همراه داراي نوعي باطري بسيار ريز با عمر دست كم 50 ساله است كه در مواقع حساس و مورد نياز براي كشور ها و سيستم هاي اطلاعاتي ناظر بر ساخت اين گوشي ها اطلاعات ارسال خواهد نمود.شاهد مثال اين قضيه نيز زماني است كه به هر دليل گوشي خودرا گم كرده و از مخابرات تقاضاي يافتنش را داشته باشيد، كه با رعايت جميع شرايط ، گوشي شما در صورت خاموش بودن نيز پيدا خواهدشد.

**راههاي امنيتي جهت كنترل و كم كردن خطرات احتمالي سوءاستفاده از گوشي تلفن همراه:**

1. از همه كد ها و رمز ها و قفل ها استفاده گردد

 **2-** از شماره گيري سريع استفاده نشود

1. توصيه مي شود از تلفن هايي با حافظه كمتر استفاده گردد مثلاًگوشي هاي ساده و ارزان قيمت
2. در هيچ موقع با دكمه و مربع بازي نكنيد. چرا كه كنجكاوي مخاطب سازمان هاي اشاره شده در بالا را در اين،كه احتمال ورود صاحب تلفن همراه به رمز يا كدي كه جنبه سري و اطلاعاتي دارد را جلب خواهد نمود

. **5-** هر از چندگاهي سيم كارت از گوشي جدا گردد و با يك فاصله زماني مجدداً استفاده گردد.

**6-** بهتر است شماره هاي مهم و حساس را در گوشي موبايل ذخيره نكنيد و ساير شماره ها را به اسامي كه خودتان متوجه مي شويد ذخيره كنيد. دست كم از اسامي به جاي نام فاميلي استفاده كنيد.

**7-** سعي كنيد تلفن همراهتان را به كسي جهت تماس قرض ندهيد، درصورت الزام به اين كار، خودتان شماره گيري نمائيد. چرا كه ممكن است طرف كدي را وارد نموده كه حساسيت بر روي شمادر خصوص كنترل و مكان يابي شما افزايش يابد.**8-** از گوشي هاي هديه شده استفاده نكنيد و قبل از هر كاري اقدام به تعويض آن نمائيد.**9-** بعد از گذشت مدت زماني مشخص گوشي خود را تعويض نمائيد.**10-** همچنين از لحاظ پزشكي توصيه مي شود در هنگام صحبت ازگوش چپ استفاده نمائيد و سعي نمائيد گوشي رو به صورت عمودي گرفته تا خطرات كمتري شما را تهديد نمايد.

**تماس تلفني با اشخاص و گرفتن مستقيم اطلاعات از آنهادر اين روش از تخليه تلفني، ابتدا پازلي تشكيل مي گردد كه گاهي براي تكميل اين پازل سال ها زمان صرف مي شود. اين پازل شامل موارد ذيل مي گردد. 1-** موضوع **2-** تشكيل گروه كار هاي مختلف مانند بررسي افراد مختلفي كه ارزش سرمايه گذاري جهت تخليه تلفني را دارند **3-** تشكيل پازل و بررسي روند تكميل پازل **4-** طرح سئوالات مختلف جهت پرسيدن از افرادي كه مد نظر قرارميگيرند**5-** رجوع به بايگاني دقيق شان، در خصوص موضوع و سابقه ي افراد**6-** جمع آوري اطلاعات آشكار در خصوص موضوعي كه از طريقرسانه هاي جمعي و نوشتاري در اختيار عموم جامعه قرار مي گيرد.**7-** هدف قرار دادن مركز اصلي اداري و ساختماني و تشكيلاتي موضوع**8-** بررسي اطلاعات موازي شامل اطلاعات اوليه و مقدماتي راجع به افراد هدف، اطلاعات اوليه و مقدماتي راجع به موضوع و نوع درگيري فرد هدف با موضوع ، پيدا كردن روش هاي اعتماد سازي،پيدا كردن سرنخ.**9-** استفاده از روانشناسي ارتباطات جهت اخذ اطلاعات.**10-** بررسي شخصيت افراد مانند ترسو بودن يا نوع زبان و لهجه طرف و. ..**11-** نحوه ي ورود به بحث **12-** نوع پوشش با عناوين مختلف و مراجع مهم كشوري مثل نهادرياست جمهوري، قوه قضائيه ، اداره ي اطلاعات، ديوان محاسبات وبه عنوان مثال گاهي جهت رسيدن به شماره موبايل يك رئيس دستگاه اجرايي، ابتدا كارمندان آن دستگاه و خانواده رئيس را بررسي ميكنند و مواردي اتفاق افتاده كه شماره موبايل رئيس يك دستگاه اجرايي را از همسر راننده آن رئيس به بهانه هاي مختلف و با استفاده از ساده لوحي اش گرفته اند. مواردي مانند نياز به تماس فوري با همسرشما كه موبايلش در دسترس نيست و نياز به شماره موبايل رييس اش داريم.

**راههاي مبارزه با تخليه تلفني و تلفن هاي مشكوك** **1-** كم كردن صحبت با تلفن.**2-** هنگام استفاده از تلفن به اين موضوع بينديشيم كه نفر سومي درحال شنيدن مكالمه مي باشد.**3-** تا كسي را نشناختيم و اطمينان حاصل ننموديم به هيچ سئوالي پاسخ ندهيم. **4-**  هيچ گونه مسائل و اطلاعات طبقه بندي شده را به صورت تلفني بازگو ننمائيم.**5-** حتي الامكان از پاسخ گويي تلفن به وسيله كودكان جلوگيري نمائيم.**6-**  آموزشهاي لازم به كودكان و اعضاي خانواده داده شود، كه به هيچ عنوان شماره تلفن يا آدرسي را به هنگام صحبت با تلفن بازگوننمايند.به هر حال تخليه تلفني روشي است نه چندان نوين، كه كاربردبسياري در خصوص مسائل امنيتي و اطلاعاتي كشور دارد و ممكن است گاهي اوقات هر يك از ما نيز جزئي از پازل تهيه شده دشمنان،جهت دريافت اطلاعات باشيم.

**تلفن همراه يا جاسوس هميشه همراه** :هر تلفن همراهي قاعدتاً داراي يك ميكروفون بسيار حساس است كه همواره قابليت فعال شدن را دارا مي باشد.فعال كردن اين ميكروفون نيازي به برقراري تماس با گوشي مزبور و فعال شدن سيم كارت گوشي و يا حتي روشن بودن تلفن همراه ندارد.امروزه يكي از تجارت هاي پرسود براي شركت هاي سازنده تلفن هاي همراه ، فروش دستگاه هاي جاسوسي يا فعال كننده ميكروفون هاي تلفن هاي همراه و امكانات شنود اين ميكروفون هاي فعال شده مي باشد.

اين دستگاه ها قابليت هايي به خريداران آنها مي دهد كه با استفاده از آن مي توانند به راحتي ، تلفن همراه شخص مورد نظر خود را به ميكروفون مخفي تبديل نموده و كليه مكالمات وي در محل كار ، منزل و يا حتي در جمع دوستان را به راحتي شنود نمايند. البته اين دستگاه هاي شنود تنها توسط شركت هاي سازنده تلفن هاي همراه ، توليد نمي شود و ساير شركت هاي توليد كننده نرم افزارهاي موبايل نيز مي توانند در صورت داشتن كد هاي نفوذ به دستگاه هاي تلفن هاي همراه شركتي خاص نرم افزار مناسب شنود اين نوع تلفن هاي همراه را توليد نمايند.البته فعال كردن اين نوع سيستم ، عموماً نياز به نصب نرم افزارمربوطه بر روي تلفن همراه افراد قرباني دارد كه اين عمل ممكن است از طريق ارسال پيامك ، بلوتوث و ... انجام گيرد.در صورتي كه فرد مهاجم بخواهد از شيوه ارسال پيامك براي نصب اين نرم افزار مخفي استفاده نمايد ، پيامكي عمومي مانند تبريك سال نوبه طيف وسيعي از مشتركان يك شهر ارسال مي كند و مشتركان تلفن هاي همراه نيز پس از خواندن اين پيامك ، فرد مهاجم را در جايگذاري اين جاسوس كوچك ياري مي رسانند.با استفاده از اين تكنولوژي ، هر تلفن همراه يك جاسوس بالقوهاست كه حتي در صورت خاموش بودن دستگاه تلفن همراه نيز ميتواند بسته به حساسيت ميكروفون خود ، امواج صوتي را از شعاعي ازمحيط خود ، جذب و ارسال نمايد.لازم به ذكر است كه اين سيستم جاسوسي ، تنها محدود به شنودمكالمات محيطي نمي شود بلكه اين دستگاه ها قادربه دسترسي به تمامي بخش هاي تلفن همراه از قبيل دوربين ، يادداشت هاي شخصي ، پيام هاي كوتاه ، ليست تماس ها و ... مي باشند.

**توصيه هايي براي مقابله با اين جاسوس خوش لباس** **:1-** در صورتي كه اين سيستم جاسوسي توسط يكي از شركت هاي سازنده تلفن همراه به فرد مهاجم فروخته شود ، عملاً هيچ كاري نمي توان انجام داد جز اينكه به هنگام حضور در جلسات كاري وخصوصي كه اطلاعات با ارزشي رد و بدل مي شود باتري موبايل خود را خارج كرده و فضاي كار را عاري از دستگاه تلفن همراه نماييد. البته برخي مدلها داراي يك باطري ريز داخلي هستند كه حتي بدون باطري هم جاسوسي خود را انجام ميدهند**2-** حتي الامكان شماره هايي كه پيامك هاي گروهي ارسال مي نمايد را **Ban** نماييد**. 3-** پيامك هايي كه از افراد ناشناس مي رسد و داراي حجمي بيش ازيك اس ام اس است را باز نكنيد**.4-** **Bluetooth** دستگاه موبايل خود را در مواقع غير ضروري ، در حالت **Off** قرار دهيد**5-**  اطلاعات شخصي و حساس مانند رمز بانكي ، شماره حساب و ...را در دستگاه تلفن همراه خود ذخيره ننماييد.**6-** در بازه هاي زماني كوتاه ، دستگاه تلفن همراه خود را **Format**نماييد.**7-** دستگاه هاي تلفن هاي همراه نسل قديم به دليل قدرت پردازش وفضاي حافظه اندك و محدود بودن نرم افزار گوشي از امنيت به مراتب بالاتري نسبت به تلفن هاي پيشرفته نسل جديد برخوردارهستند.**8-** متاسفانه شركت نوكيا بعنوان پرفروشترين گوشي ايران سابقه درخشاني در زمينه حفظ حقوق مشتريان ندارد**9-** گوشي خود را حتي براي يك لحظه در اختيار ديگران قرار ندهيد واز آن با پين كد و قفل صفحه كليد محافظت كنيد ، وارد كردن يك كد خاص كوچك فقط در عرض چند ثانيه برخي گوشي ها راتبديل به يك جاسوس هميشه همراه ميكند**10-.** در حالتهاي پيشرفته جاسوسي حتي ميتوان از طريق گوشي موبايل شخص مورد نظر را ترور كرد و يا حتي از طريق ماهواره محل دقيق هدف را مشخص كرد **11- .** دوربين گوشي را در اتاق خواب يا محل هاي خصوصي رو به ديوار يا رو به زمين بگذاريد به نحوي كه محيط در كادر دوربين قرار نگيرد **12- .** اطلاعات مهم و عكسهاي خانوادگي خود را روي گوشي ذخيره نكنيد ، سرقت ديجيتالي اطلاعات شما ، از سلام كردن و دست دادن به شما آسان تر است**13-** . برخي مدلهاي رايج و حتي ارزان قيمت بازار اين امكان را دارند كه علاوه بر دريافت بلوتوث مورد نظر ، تمام دار و ندار گوشي طرف مقابل را منتقل كنند آنقدر مسخره و آسان كه حتي تصورش هم ترس آور است **14-** . شماره تلفن شما براحتي از طريق سيستم بلوتوث قابل يافتن است پس اگر امنيت و آسايش شخصي شما مهم است در محيط هاي عمومي مانند اتوبوس و مترو بلوتوث بازي را كنار بگذاريد**15- .** هنگام شنود اصلا نيازي نيست كه گوشي شما زنگ بخورد يا به تماسي جواب بدهيد ، اينجا دنياي ديجيتال است ، شمابه راحتي شنيده ميشويدتلفن همراه شما ميتواند جاسوسي عليه شما باشد**!!Geotagging يكي از قابليتهاي موجود در تلفنهاي همراه ويژگي مشخصات جئوگرافيك تصوير GPS است كه با استفاده از گيرنده گرفته شده را ثبت ميكند.** يعني وقتي شما از يك منظره،مكان يا هر چيز ديگري عكس بگيريد طول و عرض جغرافياي محل عكسبرداري گوشي دريافت شده و در مشخصات آن عكس **GPS** توسط گيرنده ذخيره ميشود و از اين پس هر فردي كه اين تصوير را دريافت كند ثبت شده از محل عكسبرداي **Geotag** ميتواند با استفاده از مشخصات مطلع شود و آن را روي نقشه بيابد.ويژگي خوبي ميتواند باشد. مثلا دوستان **Geotagging** استفاده از شما ميتوانند از موقعيت عكسهاي كه در فليكر قرار داده ايد با خبر شوند و با ديدني هاي آنجا آشنا گردند، يا مثلاً سايتي باشد تا با خواندن تصاوير، انها را روي نقشه جمع آوري كند و با **Geotag** مشخصات استفاد ه از برنامه مديريت تصاوير مثل پيكاسا آلبوم عكسهاي خود را دسته بندي و مرتب كنيد. مي بينيد كه از خصوصيت استفاده هاي زيادي ميتوان كرد ولي اين تنها روي مثبت سكه است چون اگر هوشيار نباشيد براحتي حريم خصوصي شما را نقض خواهد كرد**. Geotagging**اطلاعات فردي و خصوصي هر شخص جز حريم خصوصيش محسوب ميشود كه حق دارد از آن دفاع كند و اجازه ورود به هر كس را ندهد از اين رو مي بينيم كه در شبكه هاي اجتماعي مانند فيس بوك افراد معمولاً اطلاعات شخصي خود را در ديد همگان قرار نميدهند تا امكان سوء استفاده فراهم نشود.حال اينگونه فرض كنيد كه اين فرد با استفاده از موبايل خود كه آن نيز فعال است تصويري از **Geotagging** دارد و قابليت **GPS** گيرنده گلهاي باغچه خانه خود ميگيرد و آن را در فيس بوكش يا وبلاگ و فليكر منتشر ميكند اين تصوير توسط دوستانش مشاهده ميشود و دست به دست ميچرخد و به اشتراك گذاشته ميشود بي خبر از آنكه به همراه آن مشخصات محل زندگيش نيز منتشر خواهد شد و هر كس ميتواند بانگاه كردن به داده هاي موجود در فايل عكس، آدرس محل زندگي او رارا براحتي پيدا كند.