یکشنبه 25 مهر 1389 - 07:52

هک موبايل و ناآگاهي کاربران

نفوذ به دنياي مجازي کاربران و استفاده از اطلاعات شخصي آنها در اينترنت به امري فراگير تبديل شده و در اين ميان هک تلفن همراه ابعاد محسوس تري پيدا کرده است اما در کشور ما به دليل ناآگاهي افراد در حال تبديل به يک معضل جدي است.

نفوذ به دنياي مجازي کاربران و استفاده از اطلاعات شخصي آنها در اينترنت به امري فراگير تبديل شده و در اين ميان هک تلفن همراه ابعاد محسوس تري پيدا کرده است اما در کشور ما به دليل ناآگاهي افراد در حال تبديل به يک معضل جدي است.
به گزارش مهر ، هک به معناي دسترسي، ايجاد تغيير و يا سوءاستفاده از اطلاعات شخصي ديگران است که امروزه به عنوان يکي از بزرگترين مشکلات دنياي ديجيتال محسوب مي‌شود و همين معضل سبب شده تا نهادها و افراد بسياري براي مقابله با خطرات و ضررهاي احتمالي آن دست بکار شوند.
فراگيرشدن اينترنت و استفاده از کامپيوترهاي شخصي از يک سو و ارائه سرويس‌هاي متنوع در بستر شبکه‌هاي محلي و جهاني از سوي ديگر باعث شده که اين روزها هکرها و يا همان دزدان ديجيتالي روزهاي خوش‌تري نسبت به دزدان دريايي سابق پيش روي خود داشته باشند.
اگرچه رعايت نکات ايمني و استفاده از نرم‌افزارهاي آنتي هک تا حدي جلوي تخريب اطلاعات کاربران مجازي را گرفته است اما شايد همين امر باعث شده باشد که هکرهاي حرفه‌اي گستره فعاليت‌هاي خود را افزايش داده و به سراغ کاربران تلفن همراه آمده باشند.
البته نقش استفاده از تکنولوژي‌هاي جديد و استفاده از اينترنت در بستر تلفن همراه را نبايد در اين بين فراموش کرد.
هک تلفن همراه هر چند به قدمت هک کامپيوترها نمي رسد اما رفته رفته با پيشرفت روزافزون امکانات تلفن همراه اين وسيله هم در معرض خطر حمله هکرها قرار دارد تا آنجا که هر فرد با داشتن نرم افزارهاي مخصوص هک به راحتي قادر خواهد بود که تلفن همراه کاربر را هک و از اطلاعات شخصي کاربران استفاده کند.

پديده هک در موبايل هاي کاربران ايراني
هک موبايل به اين معنا نيست که ديگر کاربر اختياري در کنترل تلفن همراه خود نداشته باشد بلکه بسته به نوع حمله‌اي که صورت گرفته ممکن است دفترچه تلفن و يا تمامي پيام‌هاي کوتاهي که در صندوق دريافت پيام ها (inbox) وجود دارد براي هکر ارسال شود.
در بعضي از مواقع، دزديده شدن اطلاعات شخصي کاربران به رحم و انصاف هکر مورد نظر نيز بستگي دارد چرا که در بسياري مواقع هکرهاي تلفن همراه بيشتر به دنبال عکس‌ها و حتي فيلم‌هاي شخصي افراد هستند تا دفترچه تلفن. با اين حال به اعتقاد بسياري از کارشناسان، بيشتر حملات مخرب در بخش تلفن همراه مربوط به افرادي است که تمايل زيادي به استفاده از خدمات مبتني بر GPRS دارند.
ارتباطات مخابراتي و بي سيمي، يکي از اصلي‌ترين اهدافي است که مورد توجه هکرها قرار مي‌گيرد و به اين ترتيب آنها مکالمات هر فردي را که بخواهند تحت کنترل خود مي گيرند و از اين طريق به فايل‌هاي متني، اطلاعات شخصي و حتي عکس‌هاي گرفته شده توسط تلفن همراه قرباني دست مي يابند.
در حالي که امروزه کارشناسان امنيتي بر بکارگيري راه هاي گوناگون براي مقابله با اين اقدامات هشدار مي‌دهند اما کاربران موبايل ايراني آنطور که بايد براي نفوذ افراد ناشناس بر حريم خصوصي خود نگران نيستند. چرا که به گفته باقر افخمي عضو اصلي مجتمع رسيدگي به جرائم رايانه اي و دعاوي اينترنتي دادگستري کل استان تهران تاکنون شکايتي در مورد هک موبايل به اين دادسرا ارسال نشده است.
وي دليل اين امر را بي توجهي و ناآگاهي کاربران تلفن همراه عنوان کرد و به مهر گفت: به طور قطع اين قبيل جرايم براي بسياري از کاربران صورت مي گيرد اما آنها به دليل ناآگاهي از نفوذ هکرها در تلفن همراه خود شکايتي ندارند.
باقر افخمي دعوا بر سر دامنه هاي اينترنتي و دعاوي مربوط به شرکتهاي اينترنتي با شرکتهاي مخابراتي را همچنان در صدر بيشترين موارد شکايت در بخش جرايم رايانه اي برشمرد و گفت: تنها درصد اندکي از پرونده ها مربوط به کاربران خانگي است.
با اين وجود کارشناسان معتقدند که فعاليت هکرهاي ايراني در حال حاضر فقط در نفوذ به اطلاعات شخصي کاربران خلاصه مي‌شود و همين سرک کشيدن به حريم خصوصي ديگران و انتشار اطلاعات شخصي آنها باعث شده تا امروزه شاهد گسترش نرم‌افزارهاي هک در کشور و فروش آن از طريق اينترنت باشيم.
براي روشن شدن اين موضوع کافي است جمله هک در تلفن همراه را در گوگل جستجو کرد. آن زمان است که با حجم عظيمي از وبلاگ‌ها و سايت‌هايي مواجه مي‌شويد که به صورت رايگان نرم‌افزارهاي مورد نياز را به همراه آموزش گام به گام در اختيار ناقضان حريم خصوصي مي‌گذارند. حتي اين نرم افزار با قيمت بسيار ناچيزي در حاشيه برخي خيابان هاي شهر به فروش مي رسد.
امکانات بي‌شمار نرم‌افزار هک که در بروشورهاي تبليغاتي آن عرضه شده باعث مي‌شود که ناخودآگاه از خاموش بودن بلوتوث تلفن همراه خود مطمئن باشيد.اين نرم‌افزار داراي امکاناتي نظير در اختيار گرفتن ليست شماره‌ها، sms ها ، مکالمات و پوشه‌هاي شخصي گوشي فرد هک شده است و گفته مي شود که بر روي اکثر گوشي‌هاي موبايل قابل اجرا است.

البته نفوذ به تلفن همراه هميشه از راه نصب و بكارگيري نرم‌افزار و استفاده از تكنولوژي بلوتوث خلاصه نمي‌شود. هم اكنون برخي از وبلاگ‌ها به آموزش وارد كردن كدهاي مخصوصي در گوشي فرد قرباني مي پردازند كه با استفاده از اين كدها پرداخت وجه مكالمات فرد به حساب قرباني گذاشته مي‌شود. حتي در برخي از مواقع نيز مشاهده شده كه به وسيله ارسال پيام كوتاه و يا وارد كردن يک كد مخصوص مي‌توان گوشي و سيمكارت فرد مقابل را به راحتي سوزاند!
تعميركاران تخصصي گوشي تلفن همراه معتقدند كه رايج ترين شيوه هک موبايل توسط افراد سودجو بلوتوث است. فرهاد احمدوند در اين باره گفت: هک گوشي هاي موبايل توسط برخي افراد سودجو باعث بروز مشكلات بسياري براي كاربران شده است. هكرها به راحتي از طريق هک كردن گوشي هاي تلفن همراه توسط روشن بودن بلوتوث گوشي بسته به نوع حمله مي توانند به تمامي اطلاعات شخصي افراد دسترسي داشته باشند.
وي معتقد است كه بيشترين هک موبايل در مكان هاي عمومي صورت مي گيرد چرا كه برخي از افراد با روشن كردن گوشي هاي موبايل اقدام به تبادل اطلاعات از جمله فيلم و موسيقي و غيره مي كنند. در اين صورت هكرهاي با نفوذ به راحتي مي توانند گوشي هاي موبايل را هک كنند.
با اين حال اگر كاربران تلفن همراه در زمينه استفاده از فناوري بلوتوث و GPRS از يک سو و نيز در اختيار نگذاشتن گوشي تلفن همراه خود در دسترس افراد سودجو نكات ايمني را رعايت كنند، خطري متوجه آنها نخواهد شد.
براي حفاظت در مقابل تهديدات و نفوذ به گوشي هاي موبايل رعايت برخي موارد توصيه مي‌شود:
-1 كاربران مطمئن شوند بلوتوث موبايلشان هميشه خاموش است مگر در مواردي كه خود به آن نياز دارند.
-2 حتي المقدور از هندزفري‌هاي مجهز به تكنولوژي بلوتوث استفاده نكنند.
-3 گزينه هاي موجود در قسمت بلوتوث گوشي خود را به نحوي تنظيم كنند كه براي دريافت فايل‌هاي ارسالي حداقل دو بار از آنها موافقت بخواهد.
-4 هنگام اتصال به اينترنت از طريق تلفن همراه بر روي لينک‌ها و پيام‌هاي نامطمئن كليک نكنند.
امروزه وب سايت‌هاي متعددي را مي‌توان يافت كه بازي و يا نرم‌افزارهاي رايگان را به منظور نصب بر روي تلفن همراه در اختيار كاربران قرار مي‌دهند. اين نوع نرم‌افزارها ممكن است حاوي كدهاي مخربي باشند.
توصيه مي‌شود كه كاربران هرگز از سايت‌هايي كه هويت آنها به اثبات نرسيده و نسبت به صحت و صداقت عملكرد آنها اطمينااني حاصل نشده است، نرم‌افزاري دريافت نكنند. در صورت دريافت يک فايل از يک وب سايت معتبر نيز بايد در ابتدا با استفاده از نرم‌افزارهاي آنتي ويروس آن را بررسي كرد.