

## مطلب آموزشی

### "توصیه های پلیس فتا برای جلوگیری از هک کردن موبایل"

معاونت اجتماعی پلیس فتای نیروی انتظامی با اعلام اینکه هکرها به راحتی از طریق هک کردن گوشی های تلفن همراه می توانند به تمامی اطلاعات شخصی افراد دسترسی پیدا کنند اعلام کرد که بیشتر حملات مخرب در بخش تلفن همراه مربوط به افرادی است که تمایل زیادی به استفاده از خدمات مبتنی بر GPRS دارند.

معاونت اجتماعی پلیس فضای تولید و تبادل اطلاعات ناجا در گزارشی با بیان اینکه هکرها میتوانند به راحتی از طریق هک کردن گوشی های تلفن همراه توسط روشن بودن بلوتوث گوشی به تمامی اطلاعات شخصی افراد دسترسی داشته باشند، اعلام کرد: امروزه نفوذ به دنیای مجازی کاربران و استفاده از اطلاعات شخصی آنها در اینترنت به امری فراگیر تبدیل شده و در این میان هک تلفن همراه ابعاد محسوس تری پیدا کرده است اما در کشور ما به دلیل ناآگاهی افراد در حال تبدیل به یک معضل جدی است.

براساس این گزارش، هک به معنای دسترسی، ایجاد تغییر یا سوء استفاده از اطلاعات شخصی دیگران است که امروزه به عنوان یکی از بزرگترین مشکلات دنیای دیجیتال محسوب می شود و همین معضل سبب شده تا نهادها و افراد بسیاری برای مقابله با خطرات و ضررهای احتمالی آن دست به کار شوند.

باید گفت که فراگیر شدن اینترنت و استفاده از کامپیوترهای شخصی از یک سو و ارائه سرویس های متنوع در بستر شبکه های محلی و جهانی از سوی دیگر باعث شده که این روزها هکرها یا همان دزدان دیجیتالی روزهای خوش تری نسبت به دزدان دریایی سابق پیش روی خود داشته باشند.

اگرچه رعایت نکات ایمنی و استفاده از نرم افزارهای آنتی هک تا حدی جلوی تخریب اطلاعات کاربران مجازی را گرفته است اما شاید همین امر باعث شده باشد که هکرها حرفه ای گستره فعالیت های خود را افزایش داده و به سراغ کاربران تلفن همراه آمده باشند. البته نقش استفاده از تکنولوژی های جدید و استفاده از اینترنت در بستر تلفن همراه را نباید در این بین فراموش کرد.

هک تلفن همراه هر چند به قدمت هک کامپیوترها نمی رسد اما رفته رفته با پیشرفت روزافزون امکانات تلفن همراه این وسیله هم در معرض خطر حمله هکرها قرار دارد تا آنجا که هر فرد با داشتن نرم افزارهای مخصوص هک به راحتی قادر خواهد بود که تلفن همراه کاربر را هک و از اطلاعات شخصی کاربران استفاده کند.

براساس این گزارش هک موبایل به این معنا نیست که دیگر کاربر اختیاری در کنترل تلفن همراه خود نداشته باشد بلکه بسته به نوع حمله ای که صورت گرفته ممکن است دفترچه تلفن یا تمامی پیام های کوتاهی که در صندوق دریافت پیامها (inbox) وجود دارد برای هکر ارسال شود.

در بعضی از مواقع، دزدیده شدن اطلاعات شخصی کاربران به رحم و انصاف هکر مورد نظر نیز بستگی دارد چرا که در بسیاری مواقع هکرها تلفن همراه بیشتر به دنبال عکس ها و حتی فیلم های شخصی افراد هستند تا دفترچه تلفن. با این حال به اعتقاد بسیاری از کارشناسان، بیشترین حملات مخرب در بخش تلفن همراه مربوط به افرادی است که تمایل زیادی به استفاده از خدمات مبتنی بر GPRS دارند.

ارتباطات بی سیمی مورد توجه هکرها

ارتباطات مخابراتی و بی‌سیم، یکی از اصلی‌ترین اهدافی است که مورد توجه هکرها قرار می‌گیرد و به این ترتیب آنها مکالمات هر فردی را که بخواهند تحت کنترل خود می‌گیرند و از این طریق به فایل‌های متنی، اطلاعات شخصی و حتی عکس‌های گرفته شده توسط تلفن همراه قربانی دست می‌یابند. در حالی که امروزه کارشناسان بر بکارگیری راه‌های گوناگون برای مقابله با این اقدامات هشدار می‌دهند اما کاربران تلفن‌های همراه ایرانی آن طور که باید برای نفوذ افراد ناشناس بر حریم خصوصی خود نگران نیستند.

فعالیت هک‌های ایرانی در حال حاضر فقط در نفوذ به اطلاعات شخصی کاربران خلاصه می‌شود و همین سرک کشیدن به حریم خصوصی دیگران و انتشار اطلاعات شخصی آنان باعث شده تا امروزه شاهد گسترش نرم‌افزارهای هک در کشور و فروش آن از طریق اینترنت باشیم.

برای روشن شدن این موضوع کافی است جمله هک در تلفن همراه را در گوگل جستجو کرد. آن زمان است که با حجم عظیمی از وبلاگ‌ها و سایت‌هایی مواجه می‌شوید که به صورت رایگان نرم‌افزارهای مورد نیاز را به همراه آموزش گام به گام در اختیار ناقضان حریم خصوصی می‌گذارند.

بلوتوث تلفن همراه خود را خاموش کنید

امکانات بی‌شمار نرم‌افزار هک که در بروشورهای تبلیغاتی آن عرضه شده باعث می‌شود که ناخودآگاه از خاموش بودن بلوتوث تلفن همراه خود مطمئن باشید. این نرم‌افزار دارای امکاناتی نظیر در اختیار گرفتن لیست شماره‌ها، SMSها،

مکالمات و پوشه‌های شخصی گوشی فرد هک شده است و گفته می‌شود که روی اکثر گوشی‌های موبایل قابل

اجراست.

البته نفوذ به تلفن همراه همیشه از راه نصب و بکارگیری نرم‌افزار و استفاده از تکنولوژی بلوتوث خلاصه نمی‌شود.

هم‌اکنون برخی از وبلاگ‌ها به آموزش وارد کردن کدهای مخصوصی در گوشی فرد قربانی می‌پردازند که با استفاده از این کدها پرداخت وجه مکالمات فرد به حساب قربانی گذاشته می‌شود. حتی در برخی از مواقع نیز مشاهده شده که به وسیله ارسال پیام کوتاه یا وارد کردن یک کد مخصوص می‌توان گوشی و سیم‌کارت فرد مقابل را به راحتی سوزاند! رایج‌ترین شیوه هک موبایل توسط افراد سودجو بلوتوث است

همچنین تعمیرکاران تخصصی گوشی تلفن همراه معتقدند که رایج‌ترین شیوه هک موبایل توسط افراد سودجو بلوتوث است و بیشترین هک موبایل در مکان‌های عمومی صورت می‌گیرد چرا که برخی از افراد با روشن کردن گوشی‌های موبایل اقدام به تبادل اطلاعات از جمله فیلم، موسیقی و غیره می‌کنند.

در این صورت هک‌های با نفوذ به راحتی می‌توانند گوشی‌های موبایل را هک کنند. با این حال اگر کاربران تلفن همراه در زمینه استفاده از فناوری بلوتوث و GPRS از یک سو و نیز در اختیار نگذاشتن گوشی تلفن همراه خود در دسترس افراد سودجو نکات ایمنی را رعایت کنند، خطری متوجه آنان نخواهد شد.

نکات ایمنی را رعایت کنید

براساس این گزارش، افراد برای حفاظت در مقابل تهدیدات و نفوذ به گوشی‌های موبایل رعایت برخی موارد توصیه می‌شود؛ کاربران مطمئن شوند بلوتوث تلفن همراه‌شان همیشه خاموش است مگر در مواردی که خود به آن نیاز دارند، حتی المقدور از هندزفری‌های مجهز به تکنولوژی بلوتوث استفاده نکنند، هنگام اتصال به اینترنت از طریق تلفن همراه بر روی لینک‌ها و پیام‌های نامطمئن کلیک نکنند.

منبع خبر: ایسنا