پیامک‌های خود را به‌وسیله Pc مدیریت کنید

علیرضا شیرمحمدی

برای مدیریت کامپیوترهای جیبی (Pocket Pc) که بر روی اغلب آنها سیستم عامل ویندوز موبایل به صورت پیش‌فرض نصب است، نرم‌افزارهای متعددی وجود دارد که هر یک نقاط قوت و ضعف خود را دارند.

یکی از مشکلاتی که اغلب استفاده‌کنندگان از کامپیوترهای جیبی با آن روبرو هستند، نقص نرم‌افزارهای پیش‌فرض سیستم عامل ویندوز موبایل، در انتقال پیامک‌ها و تهیه نسخه پشتیبان از آنهاست و به دلیل این‌که این نرم‌افزار یکسان‌ساز (Active Sync Microsoft) تنها می‌تواند ایمیل‌ها را مدیریت کند، بنابراین کاربرانی که پیامک‌های آنها برایشان ارزشمند است و می‌خواهند از آنها پشتیبان تهیه کنند، با مشکل روبرو هستند.

از این روشرکت‌هایی اقدام به تهیه نرم‌افزارهایی در این رابطه کرده‌اند. در میان نرم‌افزارهای موجود، Jeyo Mobile Companion توانسته با بهره‌گیری از سادگی و قدرت خود، یکی از بهترین نرم‌افزارها باشد. این نرم‌افزار بر روی موبایل نصب نمی‌شود و با بهره‌گیری از ارتباطی که نرم‌افزار (Microsoft Active Sync) بین موبایل و رایانه ایجاد می‌کند، اطلاعات مورد نیاز خود را دریافت می‌کند. این نرم‌افزار دارای یک واسط کاربری است که اطلاعات دریافتی را به کاربر رایانه نشان می‌دهد و او می‌تواند از این طریق کارهایی از جمله: ارسال پیامک، دریافت پیامک، جستجو در میان پیامک‌ها، مدیریت و ویرایش پوشه‌ها

برای دسته‌بندی پیامک‌ها، مدیریت دفترتلفن، ایجاد گروه در دفترتلفن، مدیریت شماره‌های موجود در سیمکارت، مدیریت تماس‌ها، دریافت اطلاعات فنی کامپیوتر جیبی و مدیریت نرم‌افزارها و سرویس‌هایی که بر روی ویندوز موبایل در حال اجرا هستند را انجام دهد.

لازم به ذکر است قدرت این نرم‌افزار بیشتر در توانایی آن برای تهیه نسخه پشتیبان است که می‌تواند از دفتر تلفن و پیامک‌ها یک نسخه پشتیبان تهیه کرده و آن را بر روی رایانه ذخیره کند و زمانی که به آن نسخه نیاز شد می‌توان آن را دوباره روی کامپیوتر جیبی بارگذاری کرد. در نسخه جدیدتر این نرم‌افزار (نگارش ۲/۱) امکان گپ (Chat) نیز فراهم شده، بدین صورت زمانی که اقدام به گفتگو با مخاطب خود می‌کنید، این نرم‌افزار به‌صورت خودکار پیامک‌های ارسال شده به مخاطب و پیامک‌های دریافتی از سوی مخاطب را به‌صورت مدیریت شده زیر هم قرار می‌دهد. به‌طوری که محیطی همانند محیط‌های گفتگو را برای کاربر خود تداعی کند.

دزدگیر موبایل

عکس: Ibora

پژمان عاملی‌فرد

امروز قصد معرفی برنامه‌ای را داریم که در صورت به‌سرقت رفتن گوشی شما کمک خواهد کرد تا به‌سرعت سارق را شناسایی کنید. این برنامه به دو طریق می‌تواند در ردیابی گوشی اقدام کند. یکی از طریق ارتباط ماهواره‌ای یا همان GPS و دوم از طریق ارسال پیامک. پس از به‌سرقت رفتن گوشی، کاربر می‌تواند کنترل گوشی خود را از طریق ارسال پیامک در دست بگیرد و با ارسال فرمان‌های مختلف گوشی را وادار به عکس‌العمل کند. نصب این برنامه را به کلیه دارندگان گوشی‌های دارای سیستم عامل سیمبین S60v3 توصیه می‌کنیم.

Guardian نگارش 1/03

برنامه را پس از ثبت در گوشی خود نصب کرده و وارد برنامه شوید. در بدو ورود با پیغامی مبنی بر این‌که "این سیمکارت با نامی خاص در برنامه ثبت شد" روبرو خواهید شد. این پیغام نشان‌دهنده آن است که شماره سیمکارت شما با موفقیت در برنامه ذخیره شده و شماره‌ای غیر از این شماره به‌عنوان یک سیمکارت غیر خودی شناخته می‌شود. قبل از هر چیز در دفترچه تلفن گوشی، شماره و اسم خود را وارد کنید. حال به قسمت تنظیمات یا همان Setting بروید.

در قسمت Status می‌توانید برنامه را فعال یا غیرفعال کنید. که توصیه می‌شود همیشه بر روی فعال قرار گیرد. سپس در قسمت Recipient باید شماره‌ای را وارد کنید. این شماره برای زمانیست که می‌خواهید مشخصات سارق برای این شماره ارسال گردد. در قسمت SMS text متن پیغامی را تایپ کنید که این متن می‌تواند نشان‌دهنده آن باشد که گوشی به سرقت رفته است. آنگاه در قسمت Secret code به‌دلخواه یک کد وارد کنید. این کد رمز عبور برنامه و نیز رمزیست که شما با آن می‌توانید از طریق پیامک به گوشی خود فرمان ارسال کنید. پس هیچ‌گاه آن را فراموش نکنید. در قسمت آخر که Protect Applic. Period نام دارد، یک زمان مشخص را تعیین کنید. این زمان برای آن است که اگر سیمکارت دیگری در گوشی قرار گرفت توسط این برنامه بعد از طی آن زمان خاص، یک پیامک حاوی مشخصات سیم کارت جدید گوشی برای شما ارسال گردد. پیشنهاد می‌کنیم که این گزینه را بر روی Immediately قرار دهید.

تا اینجای کار تنظیمات اصلی برنامه انجام شد. همچنین می‌توانید در قسمت Protected Application برنامه‌هایی را علامت بزنید که در صورت وارد شدن سیمکارت جدید، این برنامه‌ها قفل شوند و فقط با رمزی که در بالا قرارداده‌اید قابل دسترسی باشند. حال فرض کنید گوشی شما دست شخص دیگری افتاده و سیمکارت جدیدی در درون گوشی قرار داده شده است. بعد از روشن شدن گوشی، شماره سیمکارت جدید برای شما ارسال می‌شود که حاوی مشخصاتی از جمله کشور و یا منطقه‌ای که گوشی روشن شده است، شماره سریال گوشی و چندین مشخصات دیگر است. باید توجه داشته باشید که سارق هیچ‌گاه متوجه ارسال پیامک از طریق گوشی شما نمی‌شود. پس راحت به‌کار خود ادامه دهید و با استفاده از دستورات زیر اقدام به ارسال پیامک برای سیمکارت جدید کنید. اگر دوست دارید برای شخص مورد نظر یک پیامک اخطار ارسال کنید به‌صورتی که شماره شما قابل رویت نباشد از دستور زیر در متن پیامک استفاده کنید:

*12345*fakesms*Nashenas; Salam jenabe Saregh:D

توجه کنید که عدد 12345 همان رمز برنامه است که شما باید از رمز خود استفاده کنید. اگر دوست دارید سارق مورد نظر را رسوا کنید از دستور زیر استفاده کنید:

*12345*alarm*time=5

گوشی شما به‌مدت ۵ دقیقه با حداکثر توان شروع به‌آژیر کشیدن می‌کند. اما اگر حتی به فکر آبروی جناب سارق هستید، می‌توانید با ارسال دستور زیر آلارم را قطع کنید:

*12345*config*disable

برای تغییر شماره‌ای که در برنامه وارد کرده اید:

*12345*config*newnumber=+39328123456

برای تغییر رمز برنامه:

*12345*config*newcode =123456

برای این‌که ۲ پیامک آخر Inbox شما برایتان ارسال شود:

*12345*forward*inbox=2

برای این‌که ۲ پیامک آخر Outbox شما برایتان ارسال شود:

*12345*forward*outbox=2

برای این‌که چهار شماره اول دفتر تلفن گوشی برایتان ارسال شود:

*12345*forward*contacts=4

برای این‌که پنج شماره آخری که با آنها تماس گرفته‌اند برایتان ارسال شود:

*12345*forward*outcalls=5

برای این‌که شش شماره آخری که با گوشی شما تماس گرفته‌اند برایتان ارسال شود:

*12345*forward*incalls=6

همچنین می‌توانید از دستورات ترکیبی نیز استفاده کنید، به‌صورتی که با ارسال یک دستور چند کار مختلف انجام شود. به دستور زیر دقت کنید:

*12345*forward*incalls=5 outcalls=5 inbox=10 outbox=10 contacts=2

این یک دستور ترکیبی بوده و قادر است همه را یکجا اجرا کند. همچنین این برنامه دارای دستورات فراوان دیگری نیز هست که این دستورات در یک فایل pdf همراه با برنامه قرارداده شده است که می‌توانید بعد از دریافت برنامه، آن را نیز مطالعه کنید. برای دریافت نسخه از برنامه از آدرس زیر استفاده کنید:

http://www.persianmobiles.com/mobile42.html

هشدار

امنیت بلوتوث

بلوتوث یکی از ناامن‌ترین پروتکل‌های ارتباطی دنیاست. البته این مساله مزیت این پروتکل به‌شمار می‌آید، مگر آن‌که کاربر ناآگاه به‌آن اعتماد کند!

در سال ۱۹۹۴ شرکت اریکسون به‌همراه چهار شرکت آی‌بی‌ام، اینتل، نوکیا و توشیبا کنسرسیومی به‌نام SIG را تشکیل دادند تا روشی را استاندارد کنند که از آن طریق بتوان گوشی‌های موبایل را بدون استفاده از کابل به دستگاه‌های دیگر وصل کرد.

از همان آغاز قرار بود که این اتصال بسیار ساده باشد و انرژی اندکی را مصرف کند، بنابراین کمترین امنیت را برای آن در نظر گرفتند؛ یعنی این پروتکل رمزنگاری و احراز هویت امنی را در خود ندارد.

با توجه به‌آن‌که بیشتر محدوده‌های فرکانسی (رادیویی، مکروویو، فروسرخ و فرابنفش) که ساخت دستگاه فرستنده/گیرنده آن ساده و ارزان باشد، پیشتر استاندارد شده و کاربردهای خاص خود را یافته بود، باند فرکانسی ۲/۴ گیگاهرتز برای آن در نظر گرفته شد.

البته این باند هم با استاندارد IEEE 802.11 تداخل دارد که با تکنیکی کوچک از مشکل آن می‌کاهند.

نخستین نگارش بلوتوث در سه کلاس برد تا ۱، ۱۰ و ۱۰۰ متری و پهنای باند تا ۱ مگابیت بر ثانیه برای انتقال داده‌ها در نظر گرفته شد که البته در عمل بخشی از آن هم به‌عنوان اطلاعات سربار هدر می‌رفت. بلوتوث ۲ (۱۰ نوامبر ۲۰۰۴) این سرعت را به ۳ مگابیت بر ثانیه و بلوتوث ۳ (۲۱ آوریل ۲۰۰۹) نیز سرعت انتقال را به بیش از این مقدار رسانید.

در مجموع می‌توان گفت که بلوتوث روش انتقال ساده و ارزانی برای اطلاعات است، اما ایمن نیست و یک نفوذگر نه‌چندان ماهر هم می‌تواند اطلاعات انتقالی را شنود و یا حتی بدون اجازه، برای دیگر کاربران ارسال کند.

همچنین ایمنی پایین این روش موجب امکان‌ناپذیری تعقیب و کشف نفوذگران می‌شود. پس در هنگام فعال بودن بلوتوث گوشی، مواظب اطلاعات خود باشید و وقتی که کار به‌خصوصی ندارید، آن را غیرفعال کنید.