٦ نکته برای حفظ امنیت موبایل

هرچه شما بیشتر از دستگاه موبایل خود استفاده کنید، باید بیشتر نیز راجع به امنیت آن نگران باشید. این مساله به خصوص درصورتی‌که شما از موبایل برای کار خود استفاده نمایید، اهمیت بیشتری پیدا می‌کند. البته به خاطر داشته باشید که در صورتی‌که موبایل شما با سرور ایمیل محل کار شما پیکربندی شده باشد، احتمالا برخی از نکات امنیتی که در این مقاله به آن اشاره می‌کنیم توسط کارفرمای شما پیاده سازی شده است.

۱- سیستم عاملی انتخاب کنید که رمزگذاری را پشتیبانی می‌نماید و از رمزگذاری آن استفاده کنید.

اگر شما واقعا به امنیت دستگاه موبایل خود اهمیت می‌دهید، باید از سیستم عامل و دستگاه موبایلی استفاده کنید که رمزگذاری مبتنی بر سخت افزار را برای حافظه های داخلی و خارجی پشتیبانی می‌نماید. از جمله چنین سیستم عامل‌هایی می‌توان به Apple iOS و RIM BlackBerry اشاره کرد. این بدان معناست که داده های ذخیره شده بر روی موبایل شما در برابر پیشرفته ترین هکرها نیز تا حد خوبی محافظت می‌گردد. بدون رمزگذاری ممکن است فردی بتواند داده های موجود بر روی دستگاه را حتی بدون در اختیار داشتن pin یا کلمه عبور نیز بازیابی نماید.

رمزگذاری کامل دستگاه در دستگاه‌های فعلی اندروید محدود است و بین تولید کنندگان مختلف، دارای تفاوت‌هایی است. گوشی-های هوشمند تجاری موتورولا قابلیت‌های رمزگذاری را بر روی اندروید ۲.۳ و اندروید ۳.x فراهم می آورند. انتظار می‌رود که در سال جاری شاهد رایانه های لوحی و گوشی‌های هوشمند اندروید ۴.x باشیم که رمزگذاری را پشتیبانی می‌نمایند.

۲- یک pin یا کلمه عبور انتخاب کنید.

فعال کردن یک کلمه عبور، pin، کد عبور یا عبارت عبور، نخستین خط دفاعی برای محافظت از محرمانگی و امنیت شماست. این کار کمک می‌کند که در صورت گم شدن، به سرقت رفتن و یا جا ماندن دستگاه در جایی، از برداشتن آن توسط دیگران و مشاهده و دستکاری در محتویات آن جلوگیری به عمل آید. معمولا در صورتی‌که رمزگذاری بر روی دستگاه فعال باشد، انتخاب کلمه عبور برای آن یک اجبار است.

اگر رمزگذاری توسط سیستم عامل پشتیبانی نشده باشد، شما باید حتما خود را ملزم به تعیین یک کلمه عبور مناسب برای دستگاه خود بدانید. زیرا اگرچه احتمالا داده های شما توسط افراد خاصی که کله عبور شما را نیز ندارند قابل بازیابی است، اما حداقل به این شکل این داده ها را در برابر برخی مجرمان محافظت خواهید کرد.

۳- از بین بردن خودکار داده ها را فعال نمایید.

اغلب سیستم عامل‌های موبایل، حذف خودکار داده های دستگاه را پس از چند بار تلاش ناموفق برای وارد کردن کلمه عبور، پشتیبانی می‌نمایند. این کار در صورتی‌که رمزگذاری توسط دستگاه پشتیبانی نشده باشد، بسیار ارزشمند است، اما برای دستگاه‌هایی که از رمزگذاری بهره می‌برند نیز می‌تواند مفید باشد. دادن فرصت نامحدود به دیگران برای حدس زدن کلمه عبور، احتمال کشف آن را بیشتر می‌کند.

از بین بردن خودکار داده ها در iOS، Windows Phone ۷ و BlackBerry پشتیبانی می‌گردد، اما اندروید برای این کار نیاز به یک برنامه متفرقه دارد.

فقط به خاطر داشته باشید که حتما از تمامی داده های خود به طور منظم یک نسخه پشتیبان تهیه کنید و از راهکاری برای بازیابی داده های خود در یک دستگاه جدید استفاده نمایید.

٤- ردیابی و مدیریت از راه دور را فعال نمایید.

پیش از اینکه گوشی یا دستگاه موبایل شما گم شده یا به سرقت رود، باید یک راهکار ردیابی و مدیریت از راه دور را برای آن تنظیم نمایید. اغلب این راهکارها به شما اجازه می‌دهند که موقعیت دستگاه را بر روی یک نقشه مشاهده کنید، هشدارهای صوتی برای کمک به پیدا کردن آن ارسال می‌نمایند و با نمایش یک پیغام تصویری به دیگران می‌گویند که چگونه آن را به شما بازگردانند. این راهکارها همچنین به شما اجازه می‌دهند که از راه دور موبایل خود را قفل کرده و یا داده های آن را پیش از دستیابی دیگران به آن، پاک کنید.

Apple برای iOS ۴.۲ و نسخه های پس از آن یک راهکار رایگان در این مورد ارائه کرده است. برای نسخه های قدیمی‌تر iOS نیز یک سرویس پولی به نام MobileMe توسط این شرکت عرضه شده بود. در مورد اندروید شما باید از یک برنامه متفرقه برای این کار استفاده نمایید. مایکروسافت نیز برای Windows Phone ۷ اقدام به عرضه سرویس رایگان Windows Live for Mobile کرده است. همچنین RIM نیز سرویس رایگان BlackBerry Protect را به این منظور عرضه کرده است.

٥- استفاده از Wi-Fi hotspot ها را محدود نمایید.

زمانی که شما از Wi-Fi hotspot هایی استفاده می‌کنید که رمزگذاری شده نیستند، تمامی ترافیک اینترنت شما از طریق بی‌سیم منتقل شده و به راحتی می‌تواند مورد نفوذ قرار گیرد. مهمترین سایت‌ها وسرویس‌ها مانند وب سایت‌های بانکی، معمولا رمزگذاری (HTTPS/SSL) خود را پیاده سازی می‌کنند که از ترافیک آنها محافظت می‌نماید. ولی اغلب ارائه دهندگان سرویس‌های ایمیل و بسیاری از سایت‌های شبکه های اجتماعی این کار را انجام نمی‌دهند. در نتیجه شنود کنندگان احتمالا می‌توانند کلمات عبور و ترافیک مربوط به این سایت‌ها را جمع آوری نمایند.

نسل سوم، نسل چهارم و اغلب ارتباطات داده ای سلولی دیگر، معمولا توسط بستر ارتباطی رمزگذاری می‌شوند. علاوه بر این، استراق سمع بر روی این نوع از ارتباطات چندان معمول نیست. در نتیجه شما باید تا جایی که می‌توانید سعی کنید از ارتباطات داده ای به جای Wi-Fi hotspot های ناامن استفاده نمایید.

اما در صورتی‌که اصرار به استفاده از Wi-Fi hotspot ها دارید، از آنهایی استفاده کنید که رمزگذاری و احراز هویت ۸۰۲.۱x را فراهم می آورند.

٦- از یک آنتی ویروس یا برنامه امنیتی استفاده نمایید.

ویروس‌ها، بدافزارها و هک بر روی دستگاه‌های موبایل کم کم در حال تبدیل شدن به یک مساله بزرگ هستند. شما باید یک برنامه امنیتی نصب کنید تا بتوانید از آلودگی و نفوذ جلوگیری نمایید. اغلب راهکارهای آنتی ویروس، ویژگی‌های دیگری را نیز در اختیار شما قرار می‌دهند که از آن جمله می‌توان به حذف داده ها از راه دور، پشتیبان گیری و تعیین موقعیت مکانی دستگاه اشاره کرد.

شرکت‌های AVG و NetQin برنامه های امنیتی رایگانی را برای اندروید عرضه کرده اند. شرکت LookOut نیز برنامه های رایگانی برای اندروید، BlackBerry و Windows Mobile ارائه کرده است. در میان برخی گزینه های تجاری نیز می‌توان به McAfee WebSecure، Kaspersky Mobile Security و Trend Micro Mobile Security اشاره کرد.

منبع : سایت ماهر