



در فضای جامعه پیشرفته امروزی تلفن همراه به یکی از لوازم ضروری زندگی تبدیل شده است. در این زمان کمتر کسی را می‌توان پیدا کرد که حداقل یک خط به همراه یک گوشی تلفن همراه نداشته باشد. در واقع تلفن همراه به یک دفتر کار و بانک اطلاعات تبدیل شده است و اطلاعات مهمی نظیر، پیامک‌های خصوصی، نشانی و شماره تلفن افراد مختلف، شماره حساب‌های بانکی و رمز آن‌ها، عکس‌های خانوادگی و موارد بسیار دیگری در آن ذخیره شده است. صاحب تلفن همراه برای حفاظت از این اطلاعات مهم باید نکات مهم امنیتی را رعایت کند که در ادامه به برخی این نکات اشاره می‌شود:

1. داشتن شماره سریال و کد حذف اطلاعات

هر گوشی تلفن همراه دارای یک شماره سریال مخصوص به خود است. این شماره به شخص کمک می‌کند تا علاوه بر این- که با مراجعه به سایت اصلی شرکت تولید کننده گوشی همراه، از اصل بودن آن مطمئن شود. در صورت مفقود یا ربوده شدن گوشی، از طریق مراجع قضایی نسبت به یافتن آن اقدام کنید. یکی از راه‌ها برای بدست آوردن شماره سریال تلفن همراه برای برخی گوشی‌ها این است که کلیدهای *#60# را به ترتیب وارد کرده و بعد کلید سبز یا تماس را فشار دهید. این شماره مختص به دستگاه شماست. در مواقعی که تلفن همراه شما به سرقت می‌رود شما می‌توانید با پشتیبان شبکه خود تماس گرفته و این کد را به آن‌ها بدهید. سپس آن‌ها قادر خواهند بود تلفن همراه شما را مسدود کنند. امکان دارد شخص دیگر نتواند تلفن خود را پس بگیرد ولی این تلفن همراه دیگر کارایی ندارد و شخص دیگری حتی اگر سیم کارت آن را عوض کند، قادر به استفاده از آن نیست.

2. موقعیت مکانی

برخی تلفن‌های همراه به گونه‌ای طراحی شده‌اند که برخی از اجزا آن‌ها به صورت خودکار شرکت خدمات دهنده تلفن همراه از مکان فعلی شما با خبر می‌کنند. افزون بر این مورد بعضی از تلفن‌های همراه مجهز به سیستم GPS هستند و این اطلاعات دقیق ممکن است در داده‌های دیگری در عکس‌ها، پیامک و جست و جوی اینترنتی که از طریق تلفن همراه انجام می‌شوند، جا سازی شده باشند.

3. رمز گذاری گوشی و سیم کارت

اکثر تلفن همراهی که در بازار وجود دارند در قسمت تنظیماتشان برای محافظت از آن چه در گوشی و حافظه آن ثبت شده است گزینه‌ای برای تعیین کلمه عبور وجود دارد. شخص با رمز گذاری تلفن همراه خود در واقع دسترسی برای افراد دیگر را غیر ممکن می‌کنند این رمز گذاری می‌تواند به صورت عدد، کلمه و یا ترکیبی از این دو یا حتی تصویری نیز باشد. همچنین برای سیم کارت‌هایی که در بازار هستند امکان رمز گذاری وجود دارد. در قسمت تنظیمات تلفن همراه با فعال کردن قفل سیم کارت یا پین کد می‌توان مانع از به کارگیری دستگاه توسط اشخاص دیگر شد.

4. ناامن‌ترین پروتکل

یکی از امکانات جانبی اکثر تلفن‌های همراه بلوتوث است؛ ولی بلوتوث یکی از ناامن‌ترین پروتکل‌های ارتباطی در دنیاست. در واقع مزیت بلوتوث این است که به راحتی می‌توان بدون سیم به گوشی دیگر متصل شده و اطلاعات را منتقل کرد و اگر کاربر از نحوه کارکرد آن مطلع باشد می‌تواند از امکانات آن استفاده کند. این فناوری در شعاع 10 متری اطلاعات را در هر دستگاهی مانند تلفن همراه و لپ‌تاب و تبلت منتقل می‌کند. در عین حال ممکن است ارتباط بلوتوث شما هک شود؛ یعنی هنگامی که بلوتوث شما روشن است و در حال انتقال اطلاعات هستید هکر از این فرصت استفاده کرده و

به راحتی به تلفن همراه شما دسترسی پیدا می‌کند. این حالت حتی برای زمانی که بلوتوث روشن است و از آن استفاده نمی‌کنید؛ نیز قابل تصویر است.

بنابر این توصیه می‌شود که هنگامی که از بلوتوث استفاده نمی‌کنید یا زمانی که در حال مکالمه هستید یا اطلاعات شخص را وارد تلفن همراه می‌کنید بلوتوث را در حالت خاموش قرار دهید و اگر می‌خواهید از بلوتوث استفاده کنید اتصال خود با گوشی دیگر را با یک رمز طولانی و امن‌تر برقرار کنید.

5. رمزگذاری برای اطلاعات مهم

معمولاً تلفن‌های همراه می‌توانند اطلاعات مهمی را در حافظه خود ذخیره کنند. این اطلاعات می‌تواند شامل عکس‌ها، کلیپ‌های ویدئویی، فایل‌های متنی، سابقه تماس‌های تلفنی، اطلاعات افراد ذخیره شده در لیست تلفن و اطلاعات شخص صاحب گوشی تلفن همراه باشد. محافظت از این اطلاعات مشکل و در عین حال مهم و ضروری است. از این رو انتخاب گوشی تلفن همراه دارای اهمیت ویژه‌ای می‌باشد؛ بنابراین سعی کنید گوشی تلفنی را انتخاب نمایید که دارای قابلیت رمزگذاری برای بخش‌های مختلف اطلاعات باشد.

6. داشتن نسخه پشتیبان

فناوری‌های نوین با وجود داشتن مزیت‌های بی‌شمار، همیشه قابل اطمینان نیستند؛ شاید برای شما هم این موضوع اتفاق افتاده باشد که تمام اطلاعات ذخیره شده بر روی تلفن همراه خود را به دلایل مختلف اعم از گم شدن تلفن یا خراب شدن آن از دست داده باشید. معمولاً کاربر حرفه‌ای از تمامی اطلاعات تلفن همراه خود یک نسخه پشتیبان دارد انواع نرم افزارهای گرفتن بک آپ یا نسخه پشتیبان در اینترنت وجود دارد. همچنین بعضی از شرکت‌های تلفن همراه برای گرفتن نسخه پشتیبان اطلاعات نرم افزاری را در سایت‌شان جهت دانلود قرار می‌دهند.