



امنیت تلفن همراه



به دنبال استقبال مردم از گوشی‌های هوشمند و گران قیمت استقبال کیف‌قاپان و سارقان هم از این گوشی‌ها بیشتر شده و در موارد بسیار زمانی که به عنوان مثال فرد در خیابان در حال مکالمه با گوشی است، فرد دیگری با موتور و یا حتی پیاده به او نزدیک شده و گوشی یا تبلت او را به راحتی و به سرعت می‌قاپد و تازه از این لحظه است که پس گرفتن دستگاه مورد نظرو سوءاستفاده از اطلاعات داخل آن اهمیتی ویژه پیدا می‌کند. معمولاً بیشتر کاربران از گوشی‌های هوشمندشان برای دسترسی به اینترنت و شبکه‌های اجتماعی استفاده کرده و انواع اطلاعات را در آن ذخیره می‌کنند. برای مثال، عکس، فیلم و اطلاعات مهمی را در گوشی خود ذخیره می‌کنند. این موضوع امنیت این دستگاه‌ها را تهدید می‌کند؛ چراکه هر دستگاهی که حاوی اطلاعات باشد، قابل نفوذ هم خواهد بود و این موضوع امنیت کاربران را تهدید می‌کند.



امنیت تلفن همراه

روش های پیشگیری

- گوشی موبایل، لپ تاپ، نت بوک و هرنوع وسیله شخصیتان را از خود دور نکنید.
- به یاد داشته باشید گوشی های همراه شما جای مناسبی برای نگهداری عکس، فیلم، و تصاویر خصوصی و خانوادگی نیست، زیرا شاهد این بوده ایم که در چند سال اخیر سارقان گوشی های همراه از شهروندان به ویژه دختران در قبال عدم انتشار تصاویر خصوصی از آنها اخاذی نموده اند. پس هرگونه اطلاعات شخصی و خصوصی خود را در حافظه های جانبی مانند هارد اکسترنال ذخیره نموده و آن را در جای امنی نگهداری نمایید.
- وقتی تلفن یا تبلت خود را در اماکن عمومی مورد استفاده قرار می دهید، خیلی مضطرب و هیجان زده نشوید.
- وقتی از وسیله شخصی خود استفاده نمی کنید، آن را در حالت قفل قرار دهید که کسی با استفاده از آن وارد حساب کاربری شما در سرویس های مختلف آنلاین و آفلاین و نرم افزارها نشود.





امنیت تلفن همراه



- وقتی از سرویس وایرلس عمومی استفاده می‌کنید، در حساب‌های کاربری حساس لاگین نکنید.
- قبل از مسافرت یک نسخه‌ی پشتیبان از اطلاعات وسیله‌ی همراه خود تهیه کنید.
- نرم‌افزارهایی که برای پیدا کردن وسایل الکترونیکی به سرقت رفته به کار می‌روند را روی تبلت و گوشی خود نصب کنید. فعال کردن قابلیت حذف اطلاعات از راه دور نیز می‌تواند مفید باشد.
- رمزگذاری دستگاه خود را طبق استانداردهای موجود (انتخاب رمزی پیچیده و غیر قابل حدس که ترکیبی از حروف، کارکتر، رقم و عددی باشد) انتخاب نمایید، تغییر رمز عبور را به صورت دوره ای انجام دهید.
- بهتر است همیشه pin کد دستگاه تلفن خود را در حال فعال انتخاب نمایید.
- ردیابی و مدیریت از راه دور را فعال کنید. از این طریق شما می‌توانید مدیریت گوشی خود را از راه دور کنترل نموده. این قابلیت می‌تواند در سرقت‌های فیزیکی گوشی تلفن همراه بسیار کارآمد باشد.
- استفاده از Wi-Fi و Blue tooth را محدود کنید. و زمانی که نیازی نیست آن را خاموش نمایید.



کلاهبرداری پیامکی

ارسال پیامک یکی از شیوه هایی است که کلاهبرداران با استفاده از شیوه های خاص و مهندسی اجتماعی (مثل برنده شدن در انواع قرعه کشی ها که امروزه خیلی شایع شده، درخواست کمک های مردمی، یا باعنوان هایی که مردم را تحت تاثیر قرار می دهد) سعی می کنند کاربر را به انجام خواسته هایشان که همان برداشت غیر مجاز از حساب بانکی است ترغیب نمایند.

مثال: پیامکی مبنی بر اینکه شما در قرعه کشی طرح هزاران لبخند و یا مسابقه های مشابه در سایر اپراتورها و..... برنده شده اید به مخاطبان ارسال می شود. افراد کلاهبردار با ترفندهای خاص افراد را به پای دستگاه های خودپرداز بانک ها کشانده و با عملیات روانی و متقلبانه اطلاعات شخصی بانکی و رمز دوم کارت وی را بدست آورده و با استفاده از این اطلاعات اقدام به اخذ وجه از حساب شخصی مالباخته می نمایند؛ باید توجه داشت که جهت واریز وجه به حساب به هر دلیلی، نیازی به حضور اشخاص در پای دستگاه عابر بانک و یادادن رمز عبور حساب به تماس گیرنده نیست.





کلاهبرداری پیامکی

روش معروف چوپان دروغگو از دیگر موارد کلاهبرداری های پیامکی است. در این روش، پیامکی برای شخص ارسال می شود مبنی بر اینکه من از روستایی در یکی از استان های کشور با شما تماس می گیریم و شغل من کشاورزی و دامداری است به هنگام کار بر روی زمین به گنج یا سکه های با ارزش برخورد کرده ام که برای فروش آن ها به کمک شما احتیاج دارم. شماره شما را با استخاره به قرآن بدست آوردم. مخاطب بی اطلاع، از روی طمع و به خاطر بدست آوردن گنج زیر خاکی و سکه با پرداخت مبلغی پول، به ظاهر صاحب این سکه ها می شود؛ ولی بعد از بررسی بیشتر متوجه خواهد شد که این سکه ها تقلبی بوده و ارزش مادی خاصی ندارند. در این روش کلاهبرداران حتی برای از بین رفتن هرگونه سوءظن از احساسات مذهبی استفاده می نمایند یا کلمات را اشتباه تایپ می کنند که شخص خواننده باور کند که این افراد بی سواد و روستایی هستند.

