سازمان بورس و اوراق بهادار
Securities & Exchange Organization

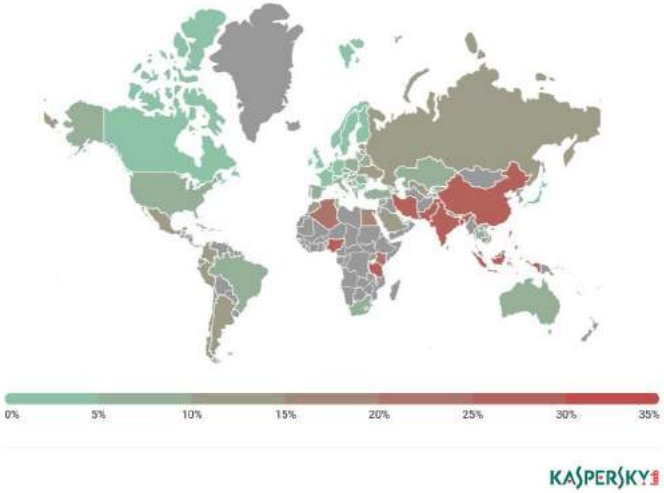
بولتن آگاهی رسانی امنیت سایبری، شماره ۷

۲۰ راهکار امن سازی گوشی‌های هوشمند

■ مرکز نظارت بر امنیت اطلاعات بازار سرمایه ■

۲۰ راهکار امن سازی گوشی‌های هوشمند

هر چه گوشی‌های هوشمند از لحاظ تکنولوژی پیشرفته‌تر می‌شود، استقبال عمومی و به‌کارگیری از آن‌ها نیز بیشتر می‌شود. اطلاعات کسب‌وکاری، حساب‌های کاربری شبکه‌های اجتماعی، ایمیل‌ها و هر نوع داده‌ای بر روی این گوشی‌های هوشمند قابل ذخیره‌سازی است. با توجه به این که اطلاعات حساس شخصی، تجاری و حتی سازمانی بر روی این گوشی‌ها ذخیره می‌شود، توجه هکرها به این گوشی‌ها بیشتر شده و در نتیجه تهدیدات امنیتی مرتبط با آن‌ها نیز افزایش می‌یابد. کافی است فکر کنید که اگر اتفاق بدی بیفتد و گوشی هوشمند شما گم و یا دزدیده شود، چه خساراتی به شما وارد می‌شود؟ طبق آمار شرکت Kaspersky، ایران سومین کشور دنیا آلوده به باج افزارهای موبایلی در سال ۲۰۱۸ شناخته شد.



ضروری است برای حفظ اطلاعات شخصی و جلوگیری از بروز خسارت‌های مادی و معنوی ناشی از افشاء اطلاعات شخصی و خصوصی، راهکارهای امن‌سازی تدوین و توسط کاربران عملیاتی شود. در این مطلب سعی بر آن است که ۲۰ راهکار امن‌سازی گوشی‌های هوشمند دارای سیستم‌عامل‌های اندروید و iOS ارائه گردد. توجه به این نکات در ارتقاء امنیت گوشی‌های هوشمندتان بسیار موثر خواهد بود.

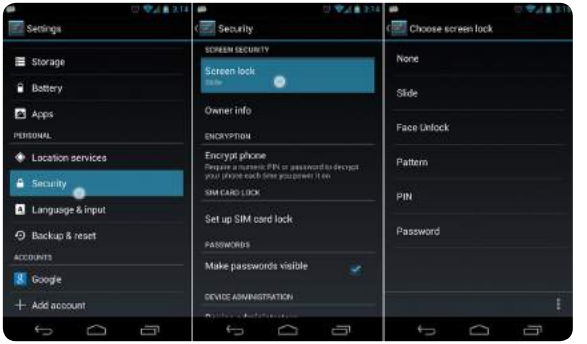
اقداماتی که می‌توان برای بهبود امنیت گوشی‌های هوشمند به کار گرفت:

۱- برای صفحه قفل گوشی خود، از کد امنیتی استفاده کنید.

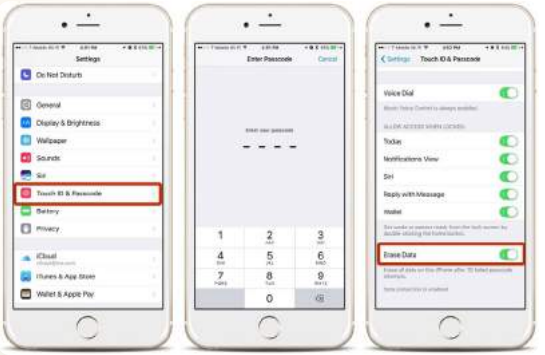
همیشه از یک PIN یا رمز عبور برای حفاظت از اطلاعات گوشی هوشمند خود استفاده کنید. اضافه کردن این لایه امنیتی به گوشی‌های هوشمند می‌تواند بسیار موثر باشد. این ممکن است واضح به نظر برسد، اما درصد بالایی از افراد، رمز عبور گوشی خود را فعال نمی‌کنند. بر اساس تحقیقات، تقریبا یک سوم مشکلات امنیتی گوشی‌های هوشمند، ناشی از عدم فعالسازی رمز عبور است. عدم فعالسازی رمز عبور، سرقت و دسترسی به اطلاعات محرمانه و خصوصی‌تان را راحت‌تر خواهد کرد. خواه شما از یک گوشی اندرویدی استفاده می‌کنید یا از یک آیفون، می‌توانید با استفاده از کد عبور یا یک الگوی امنیتی در اندروید، از دسترسی سایر افراد به موبایل خود، جلوگیری کنید. رمز مربوط به صفحه‌ی اصلی گوشی از اهمیت خاصی برخوردار است چون بسیاری از اپلیکیشن‌های مربوط به ایمیل (مثل Mail در آیفون و Gmail در اندروید) حتی گزینه‌ای برای ایجاد پسورد برای دسترسی به ایمیل‌ها، ندارند. ایمیل‌ها می‌توانند شامل اطلاعات شخصی بسیاری باشند. اغلب افراد هنگامی که در مهمانی‌ها شرکت می‌کنند، گوشی‌های خود را روی میز یا پیشخوان رها می‌کنند و این برای اشخاصی که می‌خواهند اطلاعات شما را بدست آورند، فرصت مناسبی خواهد بود.

نکته مهم: رمز ورود خود را به صورت دوره‌ای عوض کنید.

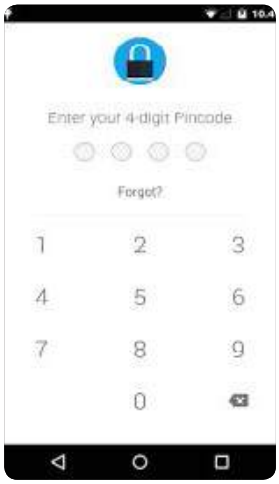
● در گوشی‌های اندروید پس از ورود به تنظیمات، مطابق مراحل ذیل می‌توانید برای گوشی رمز انتخاب کنید:



● در گوشی‌های آیفون پس از ورود به بخش تنظیمات، می‌توانید طبق مراحل ذیل passcode گوشی را فعال نمائید:



۲-بر روی اپلیکیشن‌ها، رمز بگذارید.

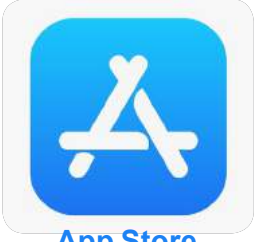


پیشنهاد می‌شود برای محافظت بیشتر از اطلاعات محرمانه خود، بر روی اپلیکیشن‌هایی که اطلاعات مهم و شخصی خود را در آن استفاده می‌کنید، رمز بگذارید. ابزارهای متعددی برای این موضوع در سیستم‌عامل‌های اندروید و iOS وجود دارد که می‌توانید از آن‌ها استفاده کنید. توصیه می‌شود رمز عبوری که بر روی اپلیکیشن‌ها ایجاد می‌کنید، متفاوت از رمز عبور ورود به گوشی هوشمندتان باشد. در تنظیمات برخی از اپلیکیشن‌ها هم در سیستم عامل iOS و هم در سیستم عامل اندروید، امکان تنظیم ورود به اپلیکیشن از طریق وارد کردن رمز وجود دارد. همچنین می‌توانید از اپلیکیشن‌هایی مانند App protector و App Lock برای رمزگذاری بر روی اپلیکیشن‌های خود استفاده نمائید.

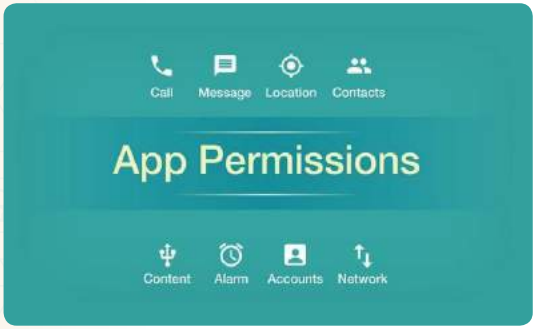
- برای توضیحات بیشتر در خصوص پیاده‌سازی این قابلیت در گوشی‌های آیفون به آدرس:
https://www.iphonelife.com/blog/32671/tip-day-how-set-touch-id-apps
و برای گوشی‌های اندروید به آدرس: https://www.androidpit.com/lock-individual-apps-on-smartphone مراجعه فرمائید.

۳-اپلیکیشن‌های مورد نیاز خود را از منابع اصلی و قابل اعتماد دانلود نمائید.

شما می‌توانید برای اطمینان بیشتر از سالم و امن بودن اپلیکیشن‌های مورد نیازتان، آن‌ها را از منابع معتبر دانلود و نصب نمائید. بهتر است قبل از دانلود یک اپلیکیشن، با توجه به نظرات نوشته شده در خصوص آن، آن را از نظر کیفیت و رتبه بندی بررسی کنید. همچنین بررسی نرم افزار از نظر سیاست حفظ حریم خصوصی نیز از دیگر نکاتی است که باید به آن توجه کنید. بسیاری از بدافزارهای اندروید به دلیل نصب اپلیکیشن از منابع نامعتبر به وجود می‌آید. امکان وجود اپلیکیشن آلوده به بدافزار در Google Play Store کم است. قابلیت Google Play Protect به طور مداوم اپلیکیشن‌ها را در حین نصب اسکن می‌کند. بنابراین اپلیکیشن‌های مورد نیاز اندرویدی خود را از Google Play Store و اپلیکیشن‌های سیستم‌عامل iOS را از App Store دانلود و نصب نمائید.



٤- مجوزهای دسترسی نرم افزار را بررسی نمائید.



دسترسی‌های مورد نیاز اپلیکیشن‌ها را بررسی کنید. در صورت مشاهده نیاز به دسترسی‌های غیر ضروری در یک اپلیکیشن، به آن اپلیکیشن مشکوک شوید. شما می‌توانید انتظار داشته باشید که یک اپلیکیشن پیام‌رسان، دسترسی ارسال و دریافت پیام متنی را داشته باشد همانطور که یک اپلیکیشن نقشه، دسترسی به موقعیت GPS نیاز داشته باشد. اما اگر یک اپلیکیشن ماشین حساب به دسترسی شبکه‌ای یا دسترسی به مخاطبین نیاز داشته باشد، باید با احتیاط با آن برخورد کنید و در صورت لزوم آن را حذف نمائید.

- برای مدیریت دسترسی‌های یک اپلیکیشن به آدرس‌های زیر مراجعه نمائید:

برای گوشی‌های آیفون: https://www.imore.com/how-manage-privacy-settings-iphone-and-ipad

برای گوشی‌های اندروید: https://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0

٥- یک آنتی ویروس خوب دانلود کنید.

استفاده از یک آنتی ویروس قدرتمند و مفید در عین ضرورت یک گام مهم و اساسی در حفظ اطلاعات محسوب می‌شود؛ پس هرچه سریعتر برای نصب یک آنتی ویروس قوی اقدام کنید. نرم افزارهای آنتی ویروس زیادی برای گوشی‌های هوشمند وجود دارد، نرم افزارهایی از قبیل Avast Mobile Security & Antivirus و Norton Mobile Security و غیره. نکته مهم در استفاده از نرم افزار آنتی ویروس، به‌روزرسانی مداوم آن و فعالسازی اکثر قابلیت‌های آن است.

٦- از وای‌فای‌های عمومی استفاده نکنید.

بهتر است تا جایی که می‌توانید از استفاده از وای‌فای عمومی اجتناب کنید. شما هرگز نمی‌توانید مطمئن شوید که در این شبکه رایگان، یک هکر یا نفوذگر کمین نکرده است. همچنین اطمینان حاصل کنید که تلفن همراه شما به صورت خودکار به شبکه‌های وای فای رایگان متصل نمی‌شود.

۷- تنظیمات بلوتوث تلفن همراهتان را به درستی پیکربندی کنید.

برای این کار به تنظیمات بلوتوث رفته در آنجا عبارت «Non-discoverable» یا غیر قابل کشف را انتخاب کنید. دلیل این کار این است که اگر بلوتوث در همه جا قابل رویت باشد افراد بیشتری برای دستیابی به اطلاعات و اتصال به تلفن همراه شما تمایل پیدا می کنند.

۸- از اکانت گوگل و iCloud (فضای ابری) خود محافظت کنید.

دومین موردی که اغلب افراد به آن توجه نمی‌کنند این است که اگر کسی بتواند وارد اکانت iCloud یا گوگل شما شود، می‌تواند به بسیاری از اطلاعاتی که در حال ایجاد یا ویرایش آن‌ها از طریق گوشی هوشمند خود هستید، دسترسی پیدا کند. در این موقع لازم است که برای هر دو اکانت از تایید هویت دو مرحله‌ای (2step authentication) استفاده کنید.

- برای تایید هویت دو مرحله‌ای icloud : https://support.apple.com/en-ng/HT207198
- برای تایید هویت دو مرحله‌ای گوگل: https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en

این موضوع شاید کمی خنده‌دار به نظر برسد اما با دسترسی به اکانت Apple ID شما، دسترسی‌هایی را که به هر یک از سرویس‌های ios، از iTunes گرفته تا iCloud و iMessage انجام می‌شود، کنترل می‌کند. اگر کسی به اپل آیدی شما دسترسی پیدا کند، می‌تواند از راه دور کلیه‌ی اطلاعات آیفون، آی‌پد و کامپیوتر مک شما را سرقت و یا پاک کند. در مورد گوگل نیز به همین صورت است. اکانت گوگل‌تان، شما را به همه‌ی سرویس‌های گوگل مثل جیمیل، گوگل پلی، گوگل مپ، گوگل کلندر، پیکاسا و گوگل پلاس و... متصل می‌کند.

۹- از Jailbreak یا Root کردن گوشی هوشمند خود اجتناب کنید.

اگر شما گوشی خود را برای سرگرمی و لذت jailbreak یا root می‌کنید احتمالا از عواقب کاری که انجام می‌دهید آگاه هستید. اما اگر این کار را به خاطر مواردی که درباره‌ی آن در خبرها شنیده‌اید انجام می‌دهید یا می‌خواهید از محدودیت‌ها و تهدیدها رهایی یابید، پس باید از این کار اجتناب کنید. سیستم عامل اندروید را root و سیستم عامل iOS را جیلبریک نکنید. این فرایندی است که به شما دسترسی کامل به کل گوشی هوشمندتان را می‌دهد اما بسیاری از محافظت‌های امنیتی تعبیه شده توسط کارخانه سازنده را از بین می‌برد.

در گوشی‌های root یا jailbreak شده، امکان فعالیت ویروس‌ها بسیار ساده‌تر می‌شود.

۱۰- مراقب اپلیکیشن‌هایی که نصب می‌کنید، باشید.

این مورد در دستگاه‌های اندرویدی اهمیت بیشتری دارد. گوگل اخیرا ۵۰۰۰۰ اپلیکیشن را که به عنوان نرم‌افزار مخرب شناسایی شده بودند، حذف کرده است. باید به این نکته توجه داشته باشید که تعداد اپلیکیشن‌هایی مانند نرم‌افزارهای مخرب، ویروس‌ها یا سایر نرم‌افزارهایی که به صورت مخفیانه اطلاعات شما را به سرقت می‌برند و به گوشی شما آسیب می‌رسانند، کم نیست. این مشکل در اپ استور اپل نیز وجود دارد اما خیلی کمتر. در بررسی‌های صورت گرفته، مشخص شده که ۹۵ درصد از نرم‌افزارهای مخرب با هدف آلوده کردن دستگاه‌های اندرویدی تولید می‌شوند و همین بدافزارها توانسته‌اند بیش از ۳۲ میلیون دستگاه اندرویدی در سال ۲۰۱۲ را آلوده کنند. اگر شما دوست ندارید که از دستگاه‌های اپل استفاده کنید، اشکالی ندارد، اما واقعیت این است که اگر شما صاحب یک دستگاه اندرویدی هستید، باید هنگام دانلود برنامه‌ها دقت زیادی به خرج دهید. بررسی کنید و ببینید که آیا تولیدکنندگان این اپلیکیشن‌ها وب سایت اختصاصی دارند یا نه، چرا که در صورت داشتن وب‌سایت اختصاصی، می‌توان تا حدی به اصالت آن اپلیکیشن اعتماد نمود. به علاوه می‌توانید در گوگل درمورد اسم این اپلیکیشن‌ها نیز تحقیق کنید و نظرات کاربران را در خصوص آن مطالعه نمائید.

۱۱- از اطلاعات خود نسخه‌ی پشتیبان تهیه کنید.

اگر نسخه پشتیبانی از اطلاعات خود نداشته باشید، درصورت دزدیده شدن گوشی، همه‌ی اطلاعات آن را از دست خواهید داد. اگر بک‌آپ ایجاد شده را روی کامپیوتر شخصی و یا در فضای ابری ذخیره کنید، می‌توانید اطلاعات تلفن خود را پاک کرده و همه‌ی آن‌ها را مجددا روی گوشی جدید خود داشته باشید. به علاوه می‌توانید به وسیله iTunes، گوشی آیفون خود را با کامپیوتر همگام کنید یا اطلاعات آن را به وسیله‌ی iCloud، به فضای ابری برگردانید. در اندروید، ابزاری داخلی برای بک‌آپ گیری طراحی شده اما این ابزار نمی‌تواند مشابه ابزار طراحی شده برای iOS، از همه‌ی اطلاعات تلفن شما بک‌آپ تهیه کند. در عوض، شما باید با استفاده از اپلیکیشن‌های جانبی از گوشی خود به صورت کامل پشتیبان‌گیری کنید و یا این که با اتصال گوشی خود به کامپیوتر شخصی از اطلاعات خود نسخه پشتیبان تهیه کنید.

۱۲- سیستم‌عامل گوشی خود را بروزرسانی کنید.

همانگونه که شما به صورت منظم، آپدیت‌های امنیتی مایکروسافت را روی کامپیوتر خود نصب می‌کنید، نصب آخرین آپدیت‌های منتشر شده برای گوشی هوشمندتان نیز ضروری است. می‌توانید چند روز بعد از انتشار آپدیت جدید، صبر کنید و مطمئن شوید که با به‌روزرسانی گوشی، مشکلاتی مانند کم شدن طول عمر باتری و... برای گوشی شما ایجاد نخواهد شد و بعدا گوشی را آپدیت کنید. سیستم عامل گوشی‌های هوشمند همواره مورد حمله قرار می‌گیرد و نسخه‌های قبلی این سیستم‌عامل به حملات آسیب‌پذیر است.
نسخه‌های به‌روزرسانی سیستم‌عامل گوشی‌های هوشمند اغلب برای بهبود کارایی و امنیت آن‌ها منتشر می‌شوند. در خصوص آپدیت‌های سیستم‌عامل اندروید، کاربران وابسته به کارخانه ساخت گوشی هوشمند خود هستند. گوشی‌های اندرویدی به طور یکسان تولید نمی‌شوند و ممکن است زمان به‌روزرسانی کارخانه‌ها با هم متفاوت باشد. به هر حال، نکته مهم دانلود نمودن به‌روزرسانی‌های مربوط به سیستم عامل (چه iOS و چه اندروید) ارتقاء نسخه سیستم عامل است. این به‌روزرسانی‌ها، گوشی هوشمندتان را در برابر تهدیدات و آسیب‌پذیری‌های جدید محافظت نموده و گوشی هوشمندتان را امن نگه می‌دارد.

برای به‌روزرسانی سیستم عامل گوشی‌های آیفون به ترتیب تصاویر زیر اقدام نمائید:

برای به‌روزرسانی سیستم‌عامل اندروید مراحل ذیل را دنبال نمائید:

۱۳- وایرلس و بلوتوث را خاموش کنید.

اتصالات گوشی خود را در زمانی که به آن نیاز ندارید، خاموش کنید. در صورتی که از Wi-Fi یا Bluetooth استفاده نمی‌کنید، این اتصالات را غیر فعال کنید. علاوه بر ذخیره باتری، اتصالات شبکه منبع حمله علیه گوشی هوشمند شما هستند. شانس حمله هکرها را کم کنید. وقتی که در خانه نیستید، بهتر است که وایرلس و بلوتوث خود را خاموش کنید و اگر می‌توانید از ارتباطات 3G و 4G استفاده کنید. هر زمان که به یک شبکه‌ی بی‌سیم نامطمئن متصل شوید، به هکرها اجازه داده‌اید تا از طریق شبکه، اطلاعات شما را بررسی کنند. وقتی راجع به بلوتوث صحبت می‌کنیم، می‌بینیم که هک شدن از این طریق کمتر رواج دارد. اما زمانی به محبوبیت آن اضافه می‌شود که مردم از تکنولوژی‌هایی فراتر از هدست استفاده می‌کنند. امروزه شما ساعت‌هایی دارید که با تلفن‌تان از طریق بلوتوث در ارتباط است به

علاوه می‌توان به نرم‌افزارهای تناسب اندام و سایر مجموعه گجت‌های میزبان دیگر نیز، اشاره کرد. اگر بلوتوث روشن و قابل مشاهده باشد، راهی برای هکرها ایجاد می‌کند تا بتوانند داده‌هایی را که بین دستگاه بلوتوثی و تلفن شما رد و بدل می‌شوند را ببینند.

۱۴- مراقب پیام‌های متنی (پیامک ها) باشید.

پیام‌های متنی هدف جذابی برای بدافزارهای موبایلی هستند، بنابراین توصیه می‌شود که اطلاعات حساس خود از قبیل اطلاعات بانکی و داده‌های خصوصی خود را از طریق پیامک ارسال نکنید. از کلیک بر روی لینک‌های ارسالی از طریق پیامک خودداری نمائید. تنظیمات ارسالی برای گوشی از طریق پیامک را فعال نکنید.

۱۵- به علامت قفل در هنگام استفاده از مرورگر گوشی دقت نمائید.

آیکن قفل در نوار آدرس مرورگر نشان دهنده برقراری ارتباط در بستر امن است. زمانی که اطلاعات شخصی و یا بانکی خود در یک وب سایت وارد می‌کنید، از وجود این آیکن مطمئن شوید. وجود این آیکن نشان می‌دهد که ارتباط شما با وب سایت مد نظر بر بستر پروتکل HTTPS و به صورت رمز شده است.

۱۶- گوشی هوشمند خود را از فروشگاه‌های معتبر خریداری نمائید.

همواره توصیه می‌شود گوشی هوشمند دست دوم نخرید و همچنین توصیه می‌گردد گوشی هوشمند خود را نفروشید. در صورت ضرورت فروش، کل اطلاعات گوشی را به گونه‌ای حذف نمائید که قابل بازگشت نباشد.

- برای این کار می‌توانید از اپلیکیشن‌های معرفی شده در آدرس زیر برای گوشی‌های اندروید استفاده کنید:

https://drfone.wondershare.com/android/android-data-erase-software.html

- برای گوشی‌های آیفون نیز از اپلیکیشن‌های معرفی شده در لینک زیر استفاده نمائید:

/https://www.imyfone.com/ios-data-erase/top-professional-ios-data-wipers

۱۷- حذف اپلیکیشن‌های بلااستفاده

هر اپلیکیشنی مشکلات امنیتی خاص خود را به همراه می‌آورد. در صورتی که از یک اپلیکیشن استفاده نمی‌کنید، با حذف آن از شر خطرات امنیتی مربوط به آن راحت شوید. هر چه راه ورود کمتری به گوشی هوشمند شما وجود داشته باشد، احتمال هک شدن آن نیز کمتر خواهد بود.

۱۸- قابلیت geo-tagging (تگ گذاری جغرافیایی) را در حین ارسال پست‌های آنلاین، غیر فعال کنید.

قابلیت geo-tagging (تگ گذاری جغرافیایی) را در حین ارسال پست‌های آنلاین، غیر فعال کنید. با استفاده از این قابلیت، هکرها می‌توانند اطلاعات زیادی از جمله محل زندگی، کار و سایر اطلاعات شخصی شما به دست آورند. در ابزارهایی که از قابلیت GPS برای مسیریابی استفاده می‌کنند، هرگز محل کار و منزل خود را با نام مشخص (home، work، خانه، کار و ...) تعریف نکنید. آدرس منزل و محل کار خود را در زمره اطلاعات شخصی خود در نظر داشته باشید.

بسیاری از اپلیکیشن‌های شبکه اجتماعی گوشی‌های هوشمند قابلیت آپلود تصاویر بر روی اینترنت را دارند. مشکلی که وجود دارد این است که بسیاری از گوشی‌ها، تگ موقعیت مکانی را به فایل عکس‌ها اضافه می‌کنند. هر کسی که به طریقی عکس‌ها را مشاهده کند، متوجه موقعیت مکانی شما در آن لحظه خواهد شد. این قابلیت بر روی بسیاری از گوشی‌ها قابل حذف است.

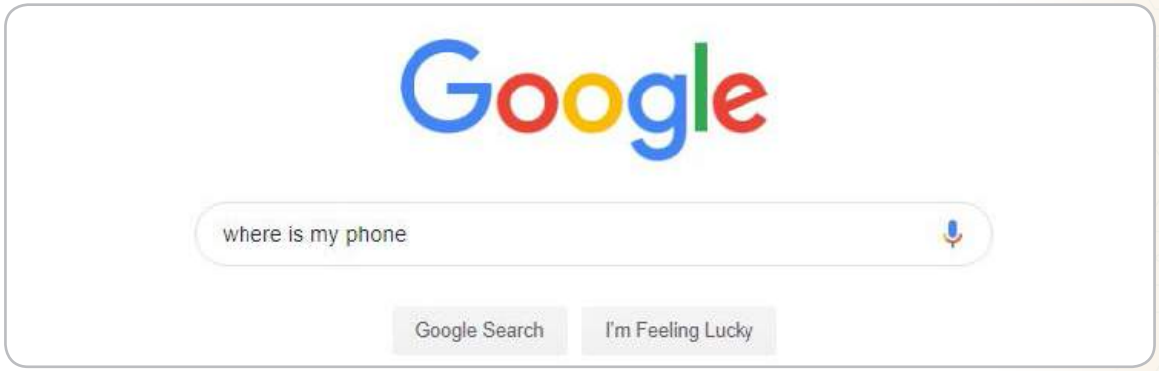
- به طور مثال برای حذف قابلیت geo-tagging در اپلیکیشن اینستاگرام به آدرس زیر مراجعه نمائید:

https://www.wikihow.com/Stop-Instagram-from-Using-Your-Location

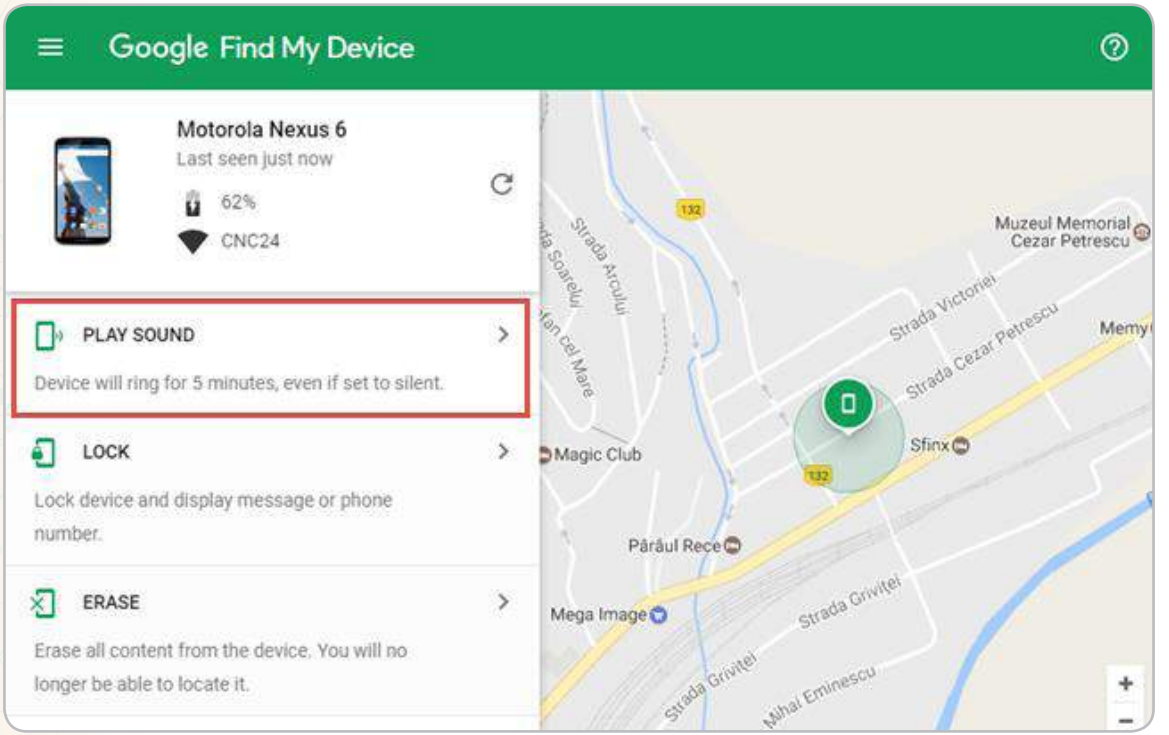
۱۹- قابلیت ردیابی موبایل را فعال کنید.

ممکن است سیستم عامل گوشی شما، گزینه Find My Phone داشته باشد که از مکانیزم‌هایی برای مانیتور کردن موقعیت گوشی‌تان استفاده می‌کند. همچنین می‌توانید با نصب برخی اپلیکیشن‌ها، این قابلیت را به گوشی خود اضافه نمائید. در سیستم عامل iOS برنامه‌ی "آیفون من را پیدا کن (Find my iPhone)"، در مایکروسافت برنامه‌ی "(Find my phone)" و در سیستم عامل اندروید برنامه "مدیریت دستگاه اندروید (Android Device Manager)" جهت ردیابی تلفن هوشمند وجود دارد.

در صورت تنظیم آدرس gmail بر روی گوشی آیفون و یا اندروید، می‌توانید با استفاده از کامپیوتر شخصی خود، ابتدا وارد حساب کاربری gmail شده و سپس عبارت زیر را در گوگل جستجو نمائید:



با کلیک بر روی نقشه نمایش داده شده، صفحه ذیل را مشاهده خواهید کرد:



در این صفحه مکان دقیق گوشی خود را می‌توانید پیدا کنید. در صورتی که گوشی شما گم شده یا به سرقت رفته است، این قابلیت قبل از خاموش شدن گوشی، بسیار موثر است. همچنین می‌توانید با کلیک بر روی گزینه Play Sound، صدای گوشی را پخش کنید.

۲۰- قابلیت remote-wipe (امحا از راه دور) را بر روی گوشی خود فعال کنید.

اگر گوشی شما به هر دلیلی ناپدید شود، با استفاده از قابلیت remote-wipe می‌توانید کل اطلاعات گوشی را فورا پاک کنید و از دسترسی افراد بدخواه به اطلاعات شخصی خود جلوگیری نمائید. با قابلیت اشاره شده در راهکار قبل (پیدا کردن گوشی از طریق گوگل) و کلیک بر روی گزینه Erase، اطلاعات گوشی را از راه دور پاک کنید.

نکته مهم: از گوشی هوشمند خود همچون رایانه شخصی خود محافظت نمائید.

توصیه های امنیتی ما را جدی بگیرید

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شمـاره ۱۳، سازمان بورس و اوراق بهادار
صنـدوق پستـی: ۶۳۶۶-۱۹۹۳۵
تلفن: ۸۴۰۸۳۵۳۵-۰۲۱ makna@seo.ir

www.seo.ir