امنیت در فضای مجازی

تهدیدهای متوجه تلفن همراه

نبض ایران
تقویت صدای ایرانیان

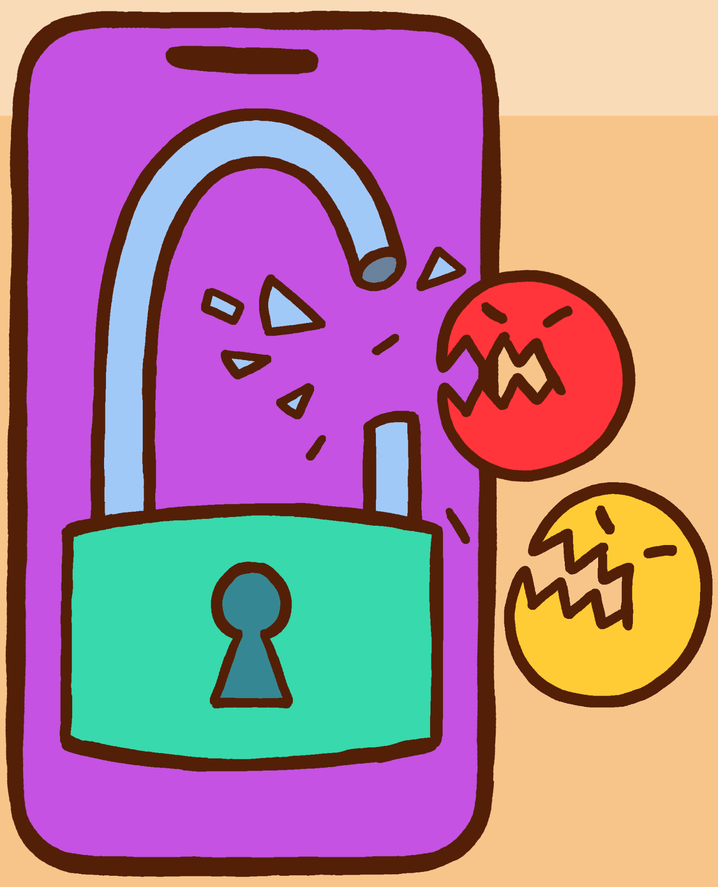
برای این که بتوانید از امنیت فردیتان حفاظت کنید باید بدانید که چه طور می‌توانید گوشی تلفن همراهتان را امن نگه دارید. برخی ملاحظات امنیتی هستند که به اوپراتورهای تلفن همراه و دیگران امکان می‌دهند تا به موقعیت مکانی و یا محتوای گوشیتان دسترسی پیدا کرده، اطلاعات حساس را برملا کنند. برخی از روش‌هایی که می‌توان از طریق آن به گوشیتان دسترسی پیدا کرد از این قرارند:

ردگیری موقعیت مکانی

مهم‌ترین راهی که اپراتورهای تلفن همراه و دیگر بازیگران می‌توانند از طریق آن موقعیت مکانی شما را پایش کنند ردگیری سیگنال گوشی تلفن همراه است. برای این کار از دکل‌های مخابراتی، دستگاه‌هایی به نام سیمولاتور مرکز موبایل، وای‌فای گوشی خودتان، سیگنال بلوتوث و یا داده‌ای که از اپ‌ها و وب‌سایت‌های دیگر نشت می‌کند استفاده می‌شود.

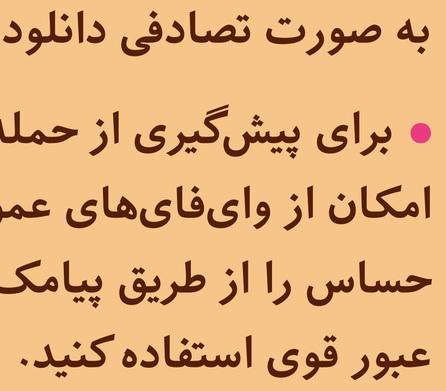
- **شرکت‌های مخابرات می‌توانند از دکل‌های تلفن همراه استفاده کنند تا از طریق سیگنال گوشی‌های تلفن همراه مکان گوشی را در فاصله حدود ۷۵۰ متری دکل ردیابی کنند. دولت‌ها می‌توانند اپراتورهای موبایل را مجبور کنند تا این اطلاعات را تحویل دهند. بدین ترتیب مقامات می‌توانند مکان فعلی و قبلی یک فرد یا مکان همه دستگاه‌های حاضر در منطقه و زمانی خاص، مانند هنگام تظاهرات را پیدا کنند. در حال حاضر، هیچ راهی برای مقابله با توانایی اپراتور برای ردیابی موقعیت مکانی گوشی تلفن همراهی که در سیستم ثبت شده و روشن باشد وجود ندارد.**
- **علاوه بر آن دولت‌ها و دیگر نهادها می‌توانند دستگاه‌هایی را به کار بگیرند که سیگنال گوشی‌های همراه را گرفته، موقعیت دقیق آن را تشخیص داده و اگر در فاصله‌ای نزدیک به گوشی باشد مکالمات آن را پایش کند. برای مقابله با این تهدید از سرویس 2G استفاده نکنید، از رومینگ فقط وقتی استفاده کنید که لازم باشد و برای مراقبت از اطلاعاتتان از ارتباطات رمزگذاری شده استفاده کنید.**
- **هنگامی که بلوتوث و وای‌فای روی دستگاهتان روشن می شود به طور خودکار سیگنالی ارسال می‌کند تا شبکه‌ها و دستگاه‌های مجاور را پیدا کند. انواع بازیگرانی که در مجاورتتان باشند می‌توانند این سیگنال را ردیابی کنند. برای پیش‌گیری از این وضعیت وقتی لازم نیست این امکانات را خاموش کنید.**

پایش تلفن

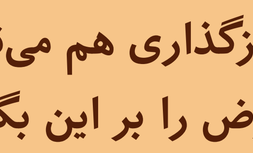


- **دستگاه گوشی تلفن همراه شما ممکن است به بدافزار آلوده شود. این کار به حمله‌کننده امکان می‌دهد تا محتوای گوشیتان را پایش کند؛ یعنی به پیامک، مکالمه تلفنی، عکس، ایمیل، تقویم و دیگر مطالب دسترسی پیدا کند. بدافزار وقتی به گوشیتان راه پیدا می‌کند که یا شما خودتان آن را به صورت تصادفی دانلود کرده باشید و یا دستگاهتان هک شده باشد.**
- **برای پیش‌گیری از حمله بدافزارها سیستم‌عامل گوشیتان را همیشه به روز نگه دارید؛ تا حد امکان از وای‌فای‌های عمومی استفاده نکنید؛ فقط از منابع مورد اعتماد اپ دانلود کنید؛ اطلاعات حساس را از طریق پیامک ارسال نکنید؛ و حتما برای محافظت از دستگاه و اطلاعاتتان از کلمه عبور قوی استفاده کنید.**
- **رمزگذاری هم می‌تواند درصدی از امنیت ایجاد کند اما معمولا به دلیل فشار دولت‌ها، ارتباطات به خوبی رمزگذاری نمی‌شود. از این رو بهتر از فرض را بر این بگذارید که ارتباطات معمول، همچون تلفن و پیامک رصد می‌شوند و تا حد امکان از اپ‌هایی استفاده کنید که ارتباطات را رمزگذاری می‌کنند.**

امنیت کاربران آیفون



- **راه‌هایی مختلف وجود دارد که از طریق آن می‌توانید خود را در برابر حملاتی که در بالا به آن اشاره شد محافظت کنید.**
- **کاربران آیفون می‌تواند حالت «Lockdown mode» را در گوشیشان فعال کنند. از این حالت تنها زمانی استفاده کنید که فکر می‌کنید هدف حمله‌ای سایبری و پیچیده قرار گرفته‌اید. تلفنی که در حال Lockdown قرار گرفته باشد طبق معمول کار نمی‌کند تا امنیت گوشی حفظ شود. در این حالت اکثر پیوست‌ها و لینک‌ها کار نخواهند کرد و فعالیت مرورگرهای اینترنت هم محدود می‌شود، دیگر نمی‌شود از طریق FaceTime با شما تماس گرفت، آلبوم‌های عکسی که دیگران با شما به اشتراک گذاشته‌اند غیر فعال می‌شود، و اگر بخواهید دستگاهتان را به شارژر یا لپ‌تاپ وصل کنید باید اول آن را Unlock کنید و تنظیمات دستگاه را هم نمی‌توانید عوض کنید.**
- **برای فعال کردن این حالت در صفحه تنظیمات (Settings) به «Privacy and security» رفته «Turn on lockdown mode» را روشن کنید.**



Lockdown Mode