SANS SECURITY AWARENESS

وای! فوریه 2018

تجهیزات همراه خود را امن کنید

مقدمه

تجهیزات همراه ابزار جالبی هستند که با استفاده از آنها به راحتی میتوان با دوستان خود در ارتباط بود، عملیات بانکی و خرید های آنلاین انجام داد، فیلم دید، بازی کرد و بسیاری از فعالیت های دیگر را انجام داد. از آنجایی که این تجهیزات بخش بسیار مهمی از زندگی شما هستند، در این مقاله چند روش ساده را ذکر میکنیم تا با استفاده از آنها تجهیزات خود را امن کنید.

تجهیزات خود را امن کنید

شاید برای شما تعجب آور باشد که بدانید بزرگترین خطر برای تجهیزات همراه نه هکرها بلکه به احتمال زیاد خود شما هستید. احتمال زیادی وجود دارد که وسیله خود را گم کنید و یا جایی فراموش کنید و بعد کسی آن را هک کرده و وارد آن وسیله شود. اولین کاری که باید برای محافظت از تجهیزات خود بکنید فعال کردن قفل شدن خودکار صفحه آن است که به آن Screenlock گفته میشود. با این کار هر زمان که نیاز داشتید وارد سیستم خود شوید ابتدا میبایست صفحه آن را با استفاده از روشهایی نظیر اثر انگشت و یا رمز های عبور قوی باز کنید. به این ترتیب اطمینان حاصل خواهید کرد که اگر دستگاه شما دزدیده شود و یا آن را را گم کنید کسی قادر نیست به محتویات آن دسترسی پیدا کند. علاوه بر این، در ذیل روشهای بیشتری را مرور میکنیم که به شما کمک میکند تا از تجهیزات خود محافظت کنید .

بروز رسانی

قابلیت بروز رسانی خودکار را در تجهیزات خود فعال کنید. به این ترتیب این تجهیزات همیشه دارای آخرین نسخه از سیستم عامل و برنامه های کاربردی خواهند بود. هکرها همیشه بدنبال جدیدترین نقاط ضعف در نرم افزارها هستند و سازندگان تجهیزات نیز دائم در حال ارائه بروز رسانی های جدید که آن نقاط ضعف را از بین ببرند. با اجرای آخرین نسخه بروز شده سیستم عامل و برنامه های موجود در تجهیزات امکان هک کردن آنها را بسیار سخت خواهید کرد.

ردیابی

برنامه هایی را که امکان ردیابی تجهیزات همراه را به شما میدهند فعال و یا اگر قبلا نصب نکرده اید آن را نصب کنید. با این روش اگر وسیله شما گم یا دزدیده شود، میتوانید از طریق اینترنت به آن متصل شده و مکان آن را بیابید، و یا در بدترین شرایط از راه دور کلیه اطلاعات موجود در آن را از بین ببرید.

برنامه های قابل اعتماد

تنها برنامه هایی را دانلود کنید که به آن نیاز دارید و حتما این کار را از طریق منابع قابل اطمینان انجام دهید. برای iPad و iPhone برنامه ها را از طریق فروشگاه شرکت اپل(Apple App Store) و برای اندروید را از گوگل پلی(Google Play) و برای تبلت های آمازون از

طریق فروشگاه آمازون(Amazon App Store) دانلود کنید. زمانیکه برنامه ها را از سایتهای غیر اصلی دانلود میکنید، عملکرد آن برنامه ها بررسی و نقد نشده و احتمال بسیاری وجود دارد که آلوده به ویروس باشند. همچنین قبل از دانلود برنامه ای حتما نظرات کاربران را در مورد آن بخوانید مطمئن شوید که بطور دایمی توسط سازنده آن بروزرسانی میشود. از استفاده از برنامه های جدید که دارای تعداد کمی نظر از طرف استفاده کنندگان هستند و یا به ندرت بروزرسانی میشوند، خودداری کنید. در آخر، جدای از اینکه برنامه را از چه منبعی دانلود کردید، در صورتیکه از آن برنامه زیاد استفاده نمیکنید، توصیه ما این است که آن را از روز دستگاه خود پاک کنید.

گزینه های حریم خصوصی

زمانیکه یک برنامه جدید را نصب میکنید، حتما گزینه های حریم خصوصی را بررسی کنید. بعنوان مثال، آیا برنامه ای که شما دانلود کردید واقعا نیاز دارد که به اطلاعات تمام دوستان و شماره تماس های شما دسترسی داشته باشد؟ توصیه دیگر ما این است که ردیابی مکانی (location Tracking) برای برنامه غیر فعال کنید، و فقط آن را برای برنامه هایی که احساس میکنید به آن نیاز دارند فعال کنید. اگر در حین استفاده از یک برنامه نسبت به نیازهای دسترسی آن راحت نیستید، سعی کنید برنامه دیگری را پیدا کنید که با شرایط شما منطبق باشد. در مجموع، بصورت دوره ای حق دسترسی های برنامه ها را چک کنید و مطمئن شوید که تغییر نکرده اند.

پشتیبان ها

همیشه از داده های خود پشتیبان بگیرید. برای تجهیزات همراه حجم زیادی از اطلاعات نظیر عکس ها و یا پیام ها، بصورت خودکار پشتیبان گیری میشوند. ولی میتوان از پیکربندی ها و برنامه ها نیز پشتیبان گرفت و به آسانی و در زمان از دست رفتن وسیله اطلاعات را بازیابی کرد و یا آن را بر روی دستگاه جدید منتقل نمود.

حین کار

در محل کار، بسیار مراقب باشید که از جاهایی که حاوی اطلاعات حساس هستند، مثل صفحه کامپیوترها و یا وایت بردها، فیلم و یا عکس نگیرید.

تجهیزات همراه شما ابزار قدرتمندی هستند، که میخواهیم از استفاده از آنها لذت ببرید. برای این کار کافیست قدمهای کوچک ذکر شده در بالا را بردارید و تا قدم بزرگی برای امن کردن خود و تجهیزات خود برداشته باشید.

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

گذرواژه ها:	https://www.sans.org/u/A3E
پشتیبان گیری/بازیابی:	https://www.sans.org/u/A3z
تخریب تجهیزات همراه:	https://www.sans.org/u/A3u
استفاده امن از برنامه های موبایل:	https://www.sans.org/u/A3p
نکته امنیتی روز:	https://www.sans.org/tip_of_the_day.php

مجوز