ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- مقدمه
- اخذ برنامه ها
- اجازه ها
- به روز رسانی برنامه ها

استفاده امن از برنامه های موبایل

مقدمه

دستگاه های قابل حمل مثل تبلت ها و گوشی های هوشمند به یکی از فن آوری های بسیار کاربردی که ما در هر دو زندگی شخصی و حرفه ای استفاده می کنیم تبدیل شده است. چیزی که دستگاه های قابل حمل را همه کاره کرده است میلیون ها برنامه ای است که می توانیم از میان آنها انتخاب کنیم. این برنامه ها در افزایش کارآیی ما، برقراری ارتباط سریع با دیگران و به اشتراک گذاری مطالب با دیگران، آموزش و تعلیم، و یا حتی سرگرمی به ما کمک میکنند. با این حال، همراه با تمام این امکانات برنامه های تلفن همراه، خطراتی هم وجود دارد. در اینجا برخی از اقداماتی که می توانید انجام دهید تا از این برنامه ها بطور امن و با خیال راحت استفاده کنید ذکر میشود.

سردبیر مهمان

کریس کراولی (Chris Crowley) مشاور مستقل، مربی مورد تایید و مولف کتب درسی SANS است. او در توییتر با نشانی **@CCrowMontance** و در Google Plus به نشانی **+ChrisCrowley** فعال است.

اخذ برنامه ها

گام اول این است که شما همیشه آنها را از منبعی امن و قابل اعتماد دانلود کنید. به یاد داشته باشید، هر کسی می تواند برنامه تلفن همراه بسازد، بنابراین باید مراقب باشید که آنها را از کجا دریافت میکنید. هکرهای اینترنتی در طی این سالها در ایجاد و توزیع برنامه های آلوده موبایل که به نظر سالم میرسند متبحر شده اند. اگر یکی از این برنامه های آلوده را نصب کنید، این هکرها می توانند کنترل دستگاه تلفن همراه شما را بدست گرفته و کارهایی از قبیل خواندن ایمیل های شما، گوش دادن به مکالمات شما و سرقت شماره تلفن ها و اطلاعات تماس روی دستگاه شما را انجام دهند. با دانلود برنامه ها تنها از منابع شناخته شده و مورد اعتماد، شانس نصب برنامه آلوده را کاهش میدهید. مارک دستگاه تلفن همراهی که استفاده می کنید تعیین کننده گزینه های شما میباشد.

برای دستگاه های اپل مانند آی پد یا آی فون، شما می توانید تنها برنامه های تلفن همراه از منبعی مدیریت شده، یعنی فروشگاه برنامه های اپل (Apple app store) دانلود کنید. مزیت این مورد این است که شرکت اپل هم خود برنامه و هم سازنده آن را بررسی میکند که مشکل امنیتی نداشته باشند. در حالی که اپل نمی تواند همه بدافزارها و افراد با نیت شوم را شناسایی کند، ولی این منبع مدیریت شده کمک می کند تا به طور چشمگیری خطر آلودگی دستگاه شما با نصب یک برنامه آلوده کاهش یابد. علاوه بر این، اگر شرکت اپل برنامه ای را در فروشگاهش یافت که باور دارد آلوده است آن را به سرعت از فهرست برنامه ها حذف خواهد کرد. تلفن های ویندوزی هم از همین روش مدیریت برنامه های مشابه استفاده میکند.

دستگاه های تلفن همراه آندرویدی متفاوت هستند. آندروید به شما انعطاف بیشتری میدهد تا بتوانید برنامه های موبایل را از هر جا در اینترنت خواستید دانلود کنید. با این انعطاف بیشتر، مسئولیت بیشتری پیش می آید. شما باید در مورد هر برنامه ای که دانلود و نصب میکنید مواظب

استفاده امن از برنامه های موبایل

کلید استفاده امن از برنامه های تلفن همراه این است که برنامه ها را فقط از منابع مورد اعتماد و مطمئن دانلود کنید و برنامه های خود را به روز رسانی کرده و اجازه دسترسی آنها را بررسی کنید.

باشید چون همه آنها موشکافی و بررسی نشده اند. گوگل نیز فروشگاه نرم افزار مدیریت شده شبیه به اپل، به نام Google Play دارد. برنامه های تلفن همراهی که شما از Google Play دانلود میکنید، بطور مختصر بررسی شده اند. به این ترتیب، توصیه میکنیم برنامه های تلفن همراه خود را برای دستگاه های اندروید فقط از Google Play دانلود کنید. از دانلود برنامه های موبایل آندروید از وب سایت های دیگر خودداری کنید، چون هر کس از جمله هکرهای اینترنتی می توانند به راحتی برنامه های تلفن همراه مخرب ایجاد و توزیع کنند، و شما را به آلوده کردن دستگاه تلفن همراه تان فریب دهند. به عنوان یک لایه حفاظت اضافی، آنتی ویروسی بر روی دستگاه تلفن همراه خود نصب کنید.

برای کاهش خطر آلودگی، برنامه هایی که جدید هستند و تعداد کمی از مردم آنها را دانلود کرده اند، و یا تعداد بسیار کمی نظرات مثبت در مورد آن نوشته اند خودداری کنید. هر چه برنامه مدت زمان بیشتری از زمان تولیدش گذشته باشد و یا نظرات مثبت بیشتری داشته باشد، احتمال اعتماد به برنامه بیشتر است. علاوه بر این، فقط برنامه هایی که نیاز دارید و استفاده میکنید را نصب کنید. از خود بپرسید، آیا من واقعا نیاز به این برنامه دارم؟ هر برنامه جدید به طور بالقوه نه تنها آسیب پذیری های جدید، بلکه مشکلات جدید حفظ حریم خصوصی نیز ارمغان می آورد. اگر دیگر از برنامه ای استفاده نمیکنید، آن را از دستگاه تلفن همراه خود حذف کنید (شما همیشه می توانید آن را دوباره نصب کنید اگر به آن نیاز پیدا کردید).

در نهایت، شما ممکن است وسوسه شوید قفل دستگاهتان را بشکنید یا به سیستم عامل دستگاه تلفن همراه خود دسترسی کامل پیدا کنید. این فرایند هک کردن آن و یا نصب برنامه تایید نشده و یا تغییر کارایی های درونی دستگاه است. ما به شدت شما را از این شکستن قفل یا دسترسی کامل به سیستم عامل بر حذر میداریم، زیرا نه تنها بسیاری از کنترل های امنیتی تعبیه شده در دستگاه تلفن همراه شما را دور می زند و یا حذف می کند، بلکه ضمانت نامه و قرارداد پشتیبانی را باطل می کند.

اجازه ها

هنگامی که برنامه تلفن همراهی را از یک منبع قابل اعتماد نصب کردید، گام بعدی این است که مطمئن شوید تنظیمهای آن امن و حریم خصوصی شما را به خطر نمی اندازد. نصب و/ یا تنظیم برنامه های تلفن همراه اغلب مستلزم آن است که شما اجازه دسترسی خاص به آنها بدهید. همیشه قبل از دادن اجازه دسترسی از خود بپرسید، آیا این برنامه واقعاً نیاز به آن اجازه برای انجام کارهایش دارد؟ به عنوان مثال، برخی از برنامه ها از خدمات تعیین محل جغرافیایی استفاده میکنند. اگر شما اجازه بدهید به برنامه که همیشه موقعیت مکانی شما را بداند، شما ممکن است به تولید کننده آن برنامه اجازه ردیابی حرکات خود را داده باشید، شاید آنها حتی این اطلاعات را به دیگران بفروشند. اگر نمی خواهید به برنامه مجوزی که درخواست میکند را بدهید، به دنبال برنامه دیگری بگردید که مطابق با نیازهای شما باشد. به یاد داشته باشید، انتخاب های زیادی دارید. دستگاه های اپل اجازه می دهند برخی از مجوزها در بخش تنظیمات دستگاه و یا در زمان اجرا تغییر دهید مانند

استفاده امن از برنامه های موبایل

دسترسی به اطلاعات مکان یابی. دستگاه های تلفن همراه ویندوز و آندروید متفاوت هستند، رویکرد آنها به شما همه یا هیچ است. اگر شما تمام مجوزهای خواسته شده برنامه را اعطا نکنید، نمی توانید برنامه را نصب کنید.

به روز رسانی برنامه ها

برنامه های موبایل، درست مثل کامپیوتر شما و سیستم عامل دستگاه همراه، باید به منظور رفع اشکالها مدام به روز شوند. مجرمان به طور مداوم در جستجو و یافتن نقاط ضعف در نرم افزارها هستند. سپس آنها از این نقاط ضعف بهره برداری میکنند. تولید کنندگان برنامه شما نیز این ضعف ها را یافته و برنامه ای برای رفع این ضعف ها و حفاظت از دستگاه شما در مقابل بهره بردای از این ضعفها میسازند. هر چه بیشتر شما نسخه های به روز رسانی را نصب میکنید، بهتر است. اکثر سیستم عامل ها به شما اجازه تنظیم سیستم برای به روز رسانی برنامه های تلفن همراه به صورت خودکار را دارند. توصیه میکنیم دستگاه را اینگونه تنظیم کنید. اگر این امکان پذیر نمی باشد، توصیه می کنیم حداقل هر دو هفته وجود نسخه به روز رسانی را بررسی کنید. درعین حال، هنگامی که برنامه های شما به روز میشوند، مجوزهای جدید که آنها ممکن است نیاز داشته باشند را بررسی کنید.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

مهندسی اجتماعی:	http://www.securingthehuman.org/ouch/2014#november2014
انهدام دستگاه تلفن همراه خود:	http://www.securingthehuman.org/ouch/2014#june2014
امن کردن تبلت جدیدتان:	http://www.securingthehuman.org/ouch/2013#december2013
اصطلاحات امنیت اطلاعات متداول:	http://www.securingthehuman.org/resources/security-terms
SEC575: دوره امنیت دستگاه تلفن همراه:	http://www.sans.org/sec575

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی