Ouch! اکتبر 2024

OUCH!

SANS SECURITY AWARENESS

ماهنامه آگاهی از امنیت اطلاعات برای شما

خطر دانلود: چگونه از برنامه های تلفن همراه مخرب پیشی بگیریم

برنامه اسرارآمیز: یک داستان هشدار دهنده کوتاه

یک یکشنبه تعطیل در حالی که سارا در رسانه های اجتماعی بود، به طور اتفاقی با تبلیغی برای یک برنامه ویرایش عکس جدید، "PiksPerfect" برخورد کرد. او که مجذوب فیلترهای خیره کننده آن شده بود، بدون تردید آن را دانلود کرد. در ابتدا، این برنامه عالی کار می کرد، اما به زودی تلفن او کند شد و تبلیغات تصادفی شروع به ظاهر شدن کردند. چند روز بعد، سارا از بانکش در مورد تراکنش‌های مشکوک هزاران دلاری تماسی دریافت کرد. او در وحشت، برنامه بانک خود را بررسی کرد و متوجه شد که پس‌اندازش تقریباً از بین رفته است. پس از گزارش کلاهبرداری و مسدود کردن حساب خود، او گیج و ناراحت شده بود.

دوستش که با فناوری آشنا بود حقیقت را کشف کرد: برنامه تلفن همراه جعلی بود و اطلاعات شخصی او از جمله جزئیات بانکی را به سرقت می برد. ماه ها طول کشید تا بهبود یابد، اما سارا محتاط تر شد و قبل از نصب برنامه های تلفن همراه، آنها را بررسی کرد. او اکنون داستان خود را به اشتراک می گذارد تا به دیگران هشدار دهد و دیگر میداند که یک لحظه بی احتیاطی می تواند عواقب گسترده ای داشته باشد.

چگونه بفهمم چه برنامه هایی ایمن هستند؟

اپلیکیشن‌های موبایل راحت و قدرتمند هستند و ما را قادر می‌سازند تا تقریباً هر کاری را در زندگی خود با لمس یک دکمه انجام دهیم. با این حال، مجرمان سایبری با ایجاد برنامه های تلفن همراه جعلی یا مخرب از این مزیت استفاده می کنند. اگر یکی از این برنامه ها را دانلود کنید، آنها می توانند تلفن شما را کنترل کنند و همه کارهای شما را زیر نظر بگیرند. کلید محافظت از خودتان این است که مطمئن شوید برنامه های تلفن همراهی که در دستگاه های خود نصب می کنید قانونی و ایمن هستند.

اول و مهمتر از همه، برنامه‌های تلفن همراه را فقط از فروشگاه‌های رسمی دانلود کنید، جایی که فروشندگان برنامه‌های تلفن همراه را بررسی می‌کنند، مانند Apple App Store یا Google Play Store. این به کاهش خطر دانلود یک برنامه تلفن همراه بد کمک می کند. فروشگاه های برنامه شخص ثالث اغلب قابل اعتماد نیستند و حتی ممکن است توسط مجرمان سایبری مدیریت شوند. اما حتی هنگام استفاده از فروشگاه برنامه های تلفن همراه قابل اعتماد، باید مراقب باشید. در اینجا چند مرحله اضافی وجود دارد که می توانید برای اطمینان از دانلود برنامه های تلفن همراه قانونی و ایمن انجام دهید.

1. نام توسعه دهنده را بررسی کنید: هنگامی که به دنبال یک برنامه موبایل خاص هستید که توسط یک شرکت خاص ایجاد شده است، مطمئن شوید که برنامه ای که دانلود می کنید توسط آن شرکت ساخته شده است. یک ترفند رایج برای کلاهبرداران، ایجاد برنامه های تلفن همراه است که بسیار شبیه به برنامه های شناخته شده هستند. نام توسعه‌دهنده را بررسی کنید - آیا همان شرکت یا یک توسعه‌دهنده معروف است یا برنامه توسط شخصی ساخته شده است که هرگز نامش را نشنیده‌اید؟ گزینه دیگر مراجعه به وب سایت رسمی برنامه یا توسعه دهنده برای یافتن پیوندهای مستقیم به برنامه تلفن همراه در فروشگاه برنامه است. این کار تضمین می کند که برنامه رسمی را دانلود می کنید.

2. بررسی ها و رتبه بندی ها را بخوانید:به نظرات و امتیازات کاربران نگاه کنید. یک برنامه قانونی دارای تعداد قابل توجهی نظرات مثبت و رتبه های بالا خواهد بود. مراقب برنامه‌هایی باشید که بررسی‌های کمی دارند، نظرات منفی زیاد، یا نظرات بیش از حد مثبت که جعلی به نظر می‌رسند.

3. تعداد دانلودها را بررسی کنید. برنامه های قانونی معمولاً تعداد دانلود بالایی دارند. یک برنامه با تعداد دانلود کم می تواند یک پرچم قرمز(هشدار) باشد.

4. بررسی مجوزها: قبل از دانلود، مجوزهایی را که برنامه درخواست می کند، مرور کنید. برنامه های قانونی فقط مجوزهای لازم برای عملکرد خود را درخواست می کنند. مراقب برنامه هایی باشید که مجوزهایی بیش از حد یا نامربوط درخواست می کنند. به عنوان مثال، آیا برنامه واقعاً نیاز به دسترسی به مخاطبین شما دارد یا همیشه مکان شما را می داند؟

5. به روز رسانی های منظم برنامه را بررسی کنید: برنامه های قانونی به طور منظم برای رفع اشکالات و بهبود عملکرد به روزرسانی می شوند. تاریخچه به‌روزرسانی برنامه را بررسی کنید تا مطمئن شوید که بروزرسانی های مکرر را دریافت می‌کند.

6. با برنامه های جدید محتاط باشید: برنامه های جدید بدون بررسی یا رتبه بندی باید با احتیاط مورد بررسی قرار گیرند. اگر برنامه قانونی باشد، احتمالاً در طول زمان نظرات و رتبه بندی‌های مثبتی به دست خواهد آورد.

پس از دانلود یک برنامه تلفن همراه، به روز رسانی خودکار را فعال کنید. اشتباهات و آسیب پذیری های جدید به طور مداوم در کد و تنظیمات برنامه های تلفن همراه یافت می شوند. با اطمینان از اینکه همیشه آخرین نسخه برنامه های تلفن همراه خود را اجرا می کنید، می توانید مطمئن شوید که این آسیب پذیری ها رفع شده اند و جدیدترین ویژگی های امنیتی را خواهید داشت. همچنین، اگر دیگر از برنامه موبایلی استفاده نمی کنید، آن را از گوشی خود حذف کنید.

سردبیر مهمان

دانیل استریمبو یک مدیر پروژه فنی در آژانس دیجیتال Travel Minds است که سابقه ای در مدیریت فناوری و عملیات دارد. او به عنوان رئیس رویدادها برای WiCyS کلرادو، به دنبال سازماندهی رویدادهای جذاب برای کمک به پیشرفت زنان در امنیت سایبری است. او دارای مدرک کارشناسی ارشد در امنیت سیستم های اطلاعاتی و مدرک تحصیلات تکمیلی در مدیریت امنیت سایبری است.

منابع

سه روشی که مهاجمان سایبری شما را هدف قرار می دهند: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/

محرکهای احساسی: چگونه مهاجمان سایبری شما را فریب میدهند: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

هر آنچه که باید درباره داده های پس زمینه بدانید: https://www.avast.com/c-what-is-background-data#

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو