بانک سینا
معاونت فناوری اطلاعات و شبکه ارتباطات
مدیریت امنیت و توسعه سیستم‌ها
اداره امنیت فناوری اطلاعات – دایره ممیزی امنیت

حریم خصوصی در تلفن همراه و شبکه‌های اجتماعی

تیرماه ۱۳۹۳

شناسنامه مستند	
عنوان/موضوع	حریم خصوصی در تلفن همراه و شبکه‌های اجتماعی
شماره/کد	SECURITYADVICE-REP-01-930429
نوع	گزارش
طبقه‌بندی	عادی

تاریخچه بازنگری

ردیف	نسخه	تهیه کننده	تاریخ تهیه	تایید کننده	تاریخ تایید	توضیحات
۱	۰۱	علیرضا مرزبانی	۱۳۹۳/۰۴/۲۹	الهه باغانی	۱۳۹۳/۰۴/۲۹	

۱. مقدمه

از آنجایی که استفاده ما از اینترنت با دستگاه‌ها و برنامه‌های جدید روبه افزایش است، فهم چگونگی کنترل حریم خصوصی حائز اهمیت می‌باشد. در این مقاله به راهنمایی‌هایی برای حفظ حریم خصوصی در هنگام استفاده از تلفن همراه و شبکه‌های اجتماعی پرداخته خواهد شد.

۲. راهنمایی‌هایی درباره حریم خصوصی در تلفن همراه

برای حفظ حریم خصوصی در هنگام استفاده از تلفن همراه باید از خود سوالاتی بپرسید. این سوالات عبارت است از:

۱- تلفن هوشمند شما چه اطلاعاتی درباره شما دارد؟

تلفن‌های هوشمند بازه وسیعی از داده‌های شخصی را شامل فهرست مخاطبین، تصاویر، تاریخچه مرورگر، یکسری اطلاعات شناسایی خاص و داده‌های مکانی ذخیره شده که طرف سومی می‌تواند به آن دسترسی داشته باشد در خود ذخیره می‌کند. تلفن خود را با استفاده از کلمه عبوری یکتا، قوی و طولانی، نرم افزارهای امنیتی و دیگر ابزارهای حفظ حریم خصوصی امن کنید.

۲- آیا دستگاه تلفن همراه شما پاک است؟

تلفن‌های هوشمند می‌توانند نسبت به ویروس‌ها و بدافزارهایی که از اطلاعات شخصی سوءاستفاده می‌کنند آسیب‌پذیر باشند. از تلفن خود با نرم‌افزارهای امنیتی و بروز رسانی سیستم‌عامل و برنامه‌های کاربردی محافظت کنید.

۳- آیا می‌دانید که مهاجمان ممکن است پیام شما را بخوانند یا ببینند؟

قبل از اینکه پیامک حاوی اطلاعات محرمانه را ارسال کنید کمی فکر کنید. در نظر داشته باشید که سوابق پیامک ها معمولاً در گوشی شما نگهداری شده و ممکن است توسط بدافزارها به سرقت بروند.

۴- آیا به حریم خصوصی دیگران احترام می‌گذارید؟

قبل از گرفتن عکس یا تصویربرداری از افراد با تلفن همراه خود، مطمئن شوید که این شخص اجازه اینکار را به شما می‌دهد. فعالیت‌هایی که به صورت آنلاین انجام می‌دهید، احتمال تاثیر گذاری روی هر کسی در محیط خانه، کار و سراسر دنیا را دارد. تمرین عادات خوب آنلاین، جامعه دیجیتالی سراسری را بهبود می‌بخشد.

۵- آیا سرویس مکان‌یابی برای برنامه‌های شما لازم است؟

بسیاری از برنامه‌های کاربردی نیاز به فعال ماندن امکان جغرافیایی (geo-location) برای فراهم کردن سرویس ندارند. محدودسازی چگونگی به اشتراک گذاری اطلاعات و فردی که با آن اطلاعات به اشتراک گذارده می‌شود امری طبیعی است.

۶- آیا درباره hotspot های WiFi چیزی می‌دانید؟

نوع کسب و کاری را که بوسیله تلفن هوشمند یا تبلت خود از طریق hotspot های WiFi انجام می‌دهید محدود کنید و تنظیمات امنیتی را روی دستگاه خود طوری تنظیم کنید تا کسانی که می‌توانند به دستگاه شما دسترسی داشته باشند محدود شوند. استفاده از hotspot ها راحت است اما می‌تواند شما را در برابر نفوذ آسیب‌پذیر کند.

۳. راهنمایی‌هایی درباره حریم خصوصی در شبکه‌های اجتماعی

برای حفظ حریم خصوصی در هنگام استفاده از شبکه‌های اجتماعی باید از خود سوالاتی بپرسید. این سوالات عبارت است از:

۱- آیا نسبت به حضور آنلاین خود اشراف دارید؟

شما نباید نسبت به تنظیمات پیشنهادی یا تنظیمات پیش فرض اعتماد کنید. درباره این تنظیمات دانش کسب کنید و سپس درباره نحوه استفاده از آنها تصمیم گیری کنید. محدودسازی به اشتراک‌گذاری اطلاعات و عدم پذیرش درخواست یک دوست امری طبیعی است.

۲- آیا می‌دانید چه کسی آنچه را که شما پست می‌کنید می‌بیند؟

در نظر بگیرید چه کسی ممکن است به پروفایل شما دسترسی داشته باشد: فامیل، دوستان، دوستان دوستان، گروه مدرسه و ... . تنظیمات امنیتی و حریم خصوصی مناسب را برای به اشتراک گذاری اطلاعات انتخاب کنید.

۳- آیا می‌دانید شهرت آنلاین شما می‌تواند به شما کمک کند؟

وجهه شخصی آنلاین قوی و مثبتی از خود ایجاد کنید. هوش، اندیشه‌ها و تسلط بر محیط دیجیتال را نشان دهید. اینکار می‌تواند در هنگام پذیرش در دانشگاه و در حین جستجو برای کار به شما کمک کند.

۴- آیا می دانید که شهرت آنلاین شما می‌تواند شما را اذیت کند؟

چیزی را که به صورت آنلاین انتشار می‌دهید، برای مدت زمانی طولانی در دسترس خواهد بود. درباره مواردی که می‌خواهید پست کنید به این بیاندیشید که می‌خواهید افراد مختلف چه اطلاعاتی را در آینده درباره شما بدانند.

۵- آیا می‌دانید حریم خصوصی شما وابسته به دوستان قابل اعتماد شما است؟

زمانی که اطلاعاتی را با هر کسی در شبکه‌های اجتماعی به اشتراک می‌گذارید، آنها می‌توانند به راحتی این اطلاعات را برای افراد دیگر بفرستند. مطمئن شوید که آنها با اطلاعات شما با مراقبت برخورد می‌کنند. از به اشتراک گذاری عکس‌ها و اطلاعاتی که امکان سوء استفاده از آنها وجود دارد خودداری کنید.

۶- آیا کلمه عبور شما طولانی، قوی و یکتا است؟

برای هر حساب کاربری آنلاین خود کلمه عبوری یکتا متشکل از حروف کوچک و بزرگ، اعداد و نشانه ایجاد کنید. کلمات عبور اطلاعات شخصی هستند که نباید به اشتراک گذارده شوند.

۷- آیا می‌دانید چه اطلاعاتی را نباید در صفحه شخصی خود به اشتراک بگذارید؟

شماره‌های تلفن، آدرس منزل، تاریخ کامل تولد، برنامه‌های سفر، آدرس پست الکترونیک، برنامه‌های کلاسی، کد ملی، کلمات عبور، اطلاعات مالی خانوادگی و شماره کارت بانکی نباید در پروفایل شما وجود داشته باشد.

قاعده طلایی در شبکه‌های اجتماعی:

فقط درباره کسانی پست بگذارید که می‌خواهید آنها درباره شما پست بگذارند.

منبع: سایت مرکز ماهر