***توصیه های امنیتی برای استفاده کودکان از تلفن همراه***

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای، نسبت به تهدیدات امنیتی در استفاده کودکان از تلفن های همراه هشدار داد و نکاتی را برای مقابله والدین با این تهدیدات اعلام کرد.

امروزه استفاده از تلفن همراه در بین کودکان در حال افزایش است؛ به همین دلیل آموزش مناسب والدین به فرزندان خود در خصوص استفاده ایمن از تلفن همراه و کنترل کردن فعالیت های کودکان می تواند تا حدی با تهدیدات امنیتی مقابله کند.

ماهر از والدین خواست تا هر زمان که فرزندانشان برای استفاده از تلفن هوشمند آماده بودند، به آنها در خصوص ایمنی و مسئولیت پذیری آموزش‌های لازم را ارائه دهند.

**دسترسی کودکان را محدود کنید**

تلفن همراه و شرکت‌های تلفن سیار (wireless company) معمولا امکاناتی را در خصوص تنظیمات حریم خصوصی و کنترل‌های ایمنی کودک ارائه می‌دهند. اکثر شرکت‌ها به والدین امکان خاموش کردن قابلیت‌هایی مانند دسترسی وب، ارسال پیام کوتاه یا دانلود کردن را می‌دهند.

برخی تلفن‌های همراه سلولی، خاص کودکان ساخته شده‌اند. این تلفن‌ها برای استفاده ساده طراحی شده‌ و دارای قابلیت‌هایی مانند دسترسی محدود به اینترنت، مدیریت دقیقه (minute management)، حفظ حریم خصوصی شماره‌ها، و دکمه‌های تماس اضطراری هستند.

**الزام استفاده از تلفن‌های محافظت شده با کلمه عبور**

کلمه عبور، کد عددی یا اثر انگشت می‌تواند منجر به عدم دسترسی مزاحمان به تلفن شود. این کار نه تنها می‌تواند از «تماس تصادفی (pocket dialing)» جلوگیری کند بلکه می‌تواند به حفظ اطلاعات و عکس‌ها در برابر دسترسی افراد غیرمجاز کمک کند.

**هنگام به اشتراک گذاری تصاویر و ویدئوها مراقب باشید**

به اشتراک گذاری و اجتماعی بودن می‌تواند فرصت‌ها و چالش هایی را ایجاد کند. این ابزارها می‌تواند باعث ایجاد خلاقیت و سرگرمی کودک شود اما از طرفی دیگر می‌تواند منجر به بروز مشکلاتی در خصوص اعتبار و ایمنی اشخاص شود.

بیشتر تلفن‌های همراه قابلیت عکس گرفتن و تصویربرداری را دارند و به اشتراک گذاری و گرفتن تصاویر را در هر لحظه آسان می‌کنند.

فرزندانتان را تشویق کنید که در خصوص حفظ حریم خصوصی خود و دیگران قبل از به اشتراک گذاری تصاویر و فیلم‌ها از طریق تلفن همراه فکر کنند.

قبل از ارسال تصاویر یا فیلم‌ها، از کسی که در تصویر یا فیلم است اجازه بگیرند. اینکه از ابتدا به اندازه کافی هوشمند باشیم که چه تصویر یا فیلمی به اشتراک گذاشته شود نسبت به اینکه بعدا بخواهیم خسارت را کنترل کنیم ساده‌تر است.

**استفاده از اپلیکیشن ها را محدود کنید**

اپلیکیشن ها و برنامه های کاربردی ممکن است اطلاعات شخصی را جمع آوری و به اشتراک بگذارند، ممکن است رایگان باشند اما فرزندان شما را ترغیب به پرداخت پول کنند و یا شامل تبلیغات باشند و به رسانه‌های اجتماعی (social medida) متصل باشند، اما این برنامه‌ها ممکن است به شما درباره کارهایی که انجام می دهند چیزی نگویند؛ براین اساس کارهایی وجود دارند که شما و فرزندتان می توانید قبل از دانلود برنامه برای یادگیری درباره برنامه های کاربردی انجام دهید.

تصاویر انتشاریافته از این برنامه را بررسی کنید، توضیحات مربوطه، رده بندی محتوایی، و نظرات کاربران را بخوانید، درباره توسعه دهنده برنامه تحقیق کنید و بررسی کنید که برنامه کاربردی چه اطلاعاتی را جمع آوری می کند.

شما می توانید چگونگی استفاده از اپلیکیشن ها توسط کودکان را محدود کنند؛ به نحوی که قبل از اینکه تلفن یا تبلت خود را به فرزندتان بدهید، به تنظیمات آن نگاه کنید.

محتوا را به آنچه که مناسب سن کودک شما است محدود کنید، کلمه عبوری را تنظیم کنید که برنامه های کاربردی بدون آن نتواند دانلود شوند و کودکان نتوانند بدون آن چیزی بخرند، همچنین خدمات داده و وای فای را خاموش کنید تا به اینترنت متصل نشوید. همچنین می توانید تلفن را در حالت پرواز قرار دهید.

درهمین حال بهترین راه برای مراقبت در قبال برنامه‌های کاربردی کودکان تست و بررسی توسط والدین است. با فرزندان خود درباره قوانین خرید و استفاده از این برنامه های کاربردی صحبت کنید.

**از حریم خصوصی کودکان خود محافظت کنید**

به کودکان خود یادآوری کنید که متن‌هایی که از افراد ناشناس دریافت می کنید نادیده بگیرند؛ یاد بگیرند که چگونه شماره هایی را در تلفن همراه خود مسدود کنند، از ارسال شماره تلفن خود به صورت آنلاین اجتناب کنند، هرگز اطلاعات شخصی یا مالی خود را در پاسخ به پیامکی ارائه ندهند.

کودکان باید پیامک هرزنامه ای را تشخیص دهند؛ به فرزندان خود در تشخیص پیامک هرزنامه ای کمک کنید و نتایج این نوع پیامک ها را توضیح دهید. این پیامک ها اغلب وعده هدایای رایگان را می دهند یا از شما خواسته می شود که اطلاعات کاربری خود را تایید کنید تا از این طریق شما اطلاعات شخصی تان را آشکار کنید؛ این پیامکها همچنین می توانند منجر به شارژ هزینه های ناخواسته در صورتحساب تلفن همراه شما شوند و می توانند کارایی تلفن همراه شما را پایین بیاورند.

**مقابله با تهدیدات امنیتی موبایل**

مرکز ماهر از خانواده ها خواست صورتحساب تلفن همراه خود را بررسی کرده و ببینند آیا هزینه های غیرمجازی در صورتحساب خود مشاهده می کنند و یا خیر. همچنین به فرزندان خود بگویند پیام هایی را که اطلاعات شخصی را درخواست می کند حذف کنند، حتی اگر وعده هدیه رایگان را می دهد.

باید توجه داشت که شرکت های قانونی اطلاعاتی مانند شماره حساب ها یا کلمات عبور را از طریق ایمیل یا متن درخواست نمی کنند؛ براین اساس به لینک هایی که در پیامک می آید پاسخ ندهید و روی آنها نیز کلیک نکنید؛ لینک ها می توانند بدافزاری را نصب کنند و شما را به سمت سایت های کلاهبرداری ببرند که اطلاعات شما را به سرقت ببرند.

منبع:

[آی‌تی اس ان](http://www.itsn.ir/?p=35438)