پنجشنبه 17 تیر 1395 - 15:25

مرکز ماهر هشدار داد؛ تهدید امنیت کودکان در شبکه‌های اجتماعی/۱۰ راهکار حفاظتی را بدانید

مرکز مدیریت امداد و هماهنگی رخدادهای رایانه‌ای با اعلام هشدار به دلیل بی احتیاطی خانواده‌ها در فضای مجازی، نکاتی را در مورد حفظ امنیت و حریم خصوصی کودکان در شبکه های اجتماعی عنوان کرد.

مرکز مدیریت امداد و هماهنگی رخدادهای رایانه‌ای با اعلام هشدار به دلیل بی احتیاطی خانواده‌ها در فضای مجازی، نکاتی را در مورد حفظ امنیت و حریم خصوصی کودکان در شبکه های اجتماعی عنوان کرد.

به گزارش خبرنگار مهر، از آنجایی که ساده ترین و کارآمدترین راهکار برای مقابله با حملات امنیتی در شبکه های اجتماعی، آموزش افراد و افزایش آگاهی آنها است، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (مرکز ماهر) در راستای آگاهی رسانی خانواده ها، در مورد خطر بی احتیاطی حضور کودکان در شبکه های اجتماعی و تهدید امنیت آنها هشدار داده است.

در گزارش مرکز ماهر، با اشاره به نمونه های سرقت اطلاعات در فضای مجازی و به ویژه شبکه های اجتماعی، ۱۰ راهکار را برای محافظت از کودکان و حفظ حریم خصوصی آنها پیشنهاد کرده است.

چگونه یک کاربر در فضای مجازی هدف حمله قرار می گیرد

بررسی ها از نحوه حملات در فضای مجازی نشان می دهد که این حملات با هدف سرقت اطلاعات و اغلب با ارسال هرزنامه به هدف موردنظر، شکل می گیرد. به نحوی که ابتدا مهاجم طعمه خود را که معمولا پیامی جعلی با ظاهری مشابه پیامکهای یک نهاد معتبر است برای تعداد زیادی کاربر ارسال می کند.

در گام بعد مهاجم منتظر می ماند به امید اینکه افراد هدف حمله، فریب خورده و خود را در دام وی گرفتار کنند. این فریب می تواند با کلیک بر روی یک پیوند و یا ارسال مشخصات فردی، اتفاق بیافتد.

در روش دیگر، طعمه گذاری مهاجم با استفاده از ابزارهای فیزیکی مانند وسایلی چون لوح فشرده (سی دی) و یا فلش که حاوی بدافزار است، اتفاق می افتد و قربانی این وسائل را به رایانه های خود متصل کرده و با این کار، بدافزار مهاجم اجرا می‌شود. به این ترتیب دسترسی مهاجم به اطلاعات موجود بر روی این رایانه ها فراهم می شود.

از دیگر روشهای مورد هدف قرار گرفتن کاربر این است که مهاجم افراد خاصی را با هدف کسب اطلاعات در مورد آنها به دام می اندازد. به نحوی که مهاجم با بازگویی اطلاعاتی که از قربانی به دست آورده، اعتماد وی را جلب می کند و به وی این‌طور تلقین می کند که دارای اشتراکات زیادی با یکدیگر هستند.

در نهایت اعتماد جلب شده از قربانی سبب می شود تا وی اطلاعاتی که در اختیار افراد غیر، قرار نمی دهد را به سادگی در اختیار مهاجم بگذارد.

با وجود روشهایی که به راحتی می تواند به سرقت اطلاعات منجر شود، کودکان در شبکه های اجتماعی می توانند نخستین گروه آسیب پذیری باشند که به راحتی هدف حمله مهاجمان قرار می گیرند.

کودکان در شبکه های اجتماعی با چه روبرو هستند؟

مطالب غیراخلاقی و دارای بدآموزی: همواره این خطر وجود دارد که در فضای مجازی و شبکه های اجتماعی با مطالبی مواجه شویم که حاوی مضامین غیراخلاقی نظیر تفکرات ضددینی، ترویج استفاده از مواد مخدر و محتوای مستهجن باشد.

در این میان باید مراقب بود تا کودکان که پیش از ورود به فضای مجازی در کانون سالم خانواده، رشد کرده اند و هنوز قدرت شناخت و تصمیم گیری درستی در مواجه با این مسائل ندارند، با این مطالب مواجه نشوند.

دوستی با افراد ناباب: در شبکه های اجتماعی افراد از هر طیف اعم از خوب و بد، حضور دارند. همانطور که والدین در زندگی

روزمره، دوستان و اطرافیان کودکان خود را زیرنظر داشته و اجازه دوستی کودکان با افراد ناباب را نمی دهند در فضای مجازی نیز باید بر ارتباط کودک خود با دیگران نظارت داشته باشند.

والدین نباید اجازه دهند که افراد ناباب و غیرقابل اعتماد با کودکان آنها دوست شده و تاثیر منفی بر اخلاق و رفتار و افکار آنان بگذارند.

سودجویابی که به دنبال فریب کودکان هستند: کودکان پاک و معصوم هستند و ذهن بی آلایشی دارند، به همین خاطر از خطرات موجود در محیط اطراف خود آگاهی کمتری داشته و ممکن است ساده تر فریب بخورند.

ممکن است در گوشه و کنار فضای مجازی و در میان انبوه مطالب موجود در شبکه های اجتماعی، کسانی با انگیزه های سوء از این عوامل استفاده کرده و برای کودکان دام پهن کرده باشند.

افشای اطلاعات شخصی بدون توجه و آگاهی: کودکان توانایی کمتری در تشخیص و تمایز میزان شرایط عادی و شرایط خطرناک دارند. یکی از مهمترین این شرایط زمانی است که در شبکه های اجتماعی و فضای مجازی، کاربران اطلاعات شخصی و خصوصی خود را در اختیار دیگران قرار می دهند.

کودکان ممکن است از روی سادگی و کودکی، فریب خورده و اطلاعات شخصی را در اختیار دیگران بگذارند. اطلاعاتی که هم حریم خصوصی خود آنان و هم امنیت خانواده را به خطر می اندازد.

۱۰ راهکار برای آنکه از کودکان تان محافظت کنید

۱. مراقب باشید کودکان کم سن بدون نظارت از شبکه های اجتماعی استفاده نکنند.

۲. تنظیمات امنیت و حریم خصوصی دستگاههای قابل اتصال و همراه را به طور مرتب بررسی کنید.

۳. تنظیمات حریم خصوصی حسابهای کاربری را به صورت مداوم بررسی کنید.

۴. از نرم افزارهای فیلترینگ و مانیتورینگ استفاده کنید.

۵. برای استفاده از شبکه های اجتماعی و دستگاههای متصل، قانون بگذارید.

۶. سعی کنید عادتهای کودکان و نوجوانان خود را بشناسید.

۷. الگوی مناسبی برای کودکانتان باشید.

۸. سعی کنید در مورد فناوریهای جدید به روز باشید.

۹. مراقب تصاویر و مطالبی که کودکانتان در شبکه های اجتماعی ارسال می کنند باشید.

۱۰. اتصال به اینترنت برای کودکان در اتاق خصوصی ممنوع!
معصومه بخشی پور