

راهاندازی شبکه اجتماعی دانش آموزی

معاون پرورشی و فرهنگی وزارت آموزش و پرورش از راهاندازی شبکه اجتماعی دانش آموزان تا پایان سال ۹۴ خبر داد و گفت: سعی می‌کنیم دانش آموزان را با ابعاد مثبت فضای مجازی آشنا و به وبلاگ نویسی، ایجاد نشریات الکترونیکی و حضور فعال در فضای مجازی تشویق کنیم.

به گزارش جام جم آنلاین حمیدرضا کفاش در گفت‌وگو با ایسنا، درباره آخرین اقدامات انجام شده درخصوص راهاندازی شبکه اجتماعی دانش آموزان اظهار کرد: مراحل مطالعاتی شبکه اجتماعی دانش آموزان با عنوان "شاد" به پایان رسیده است و اکنون در حال طی مراحل صدور مجوز است.

وی افزود: در همین راستا تفاهم‌نامه‌ای با وزارت ارتباطات و فناوری اطلاعات به عنوان یک طرح مشترک به امضا رسیده است و امیدواریم بتوانیم در سال ۹۴ شبکه اجتماعی دانش آموزان را راهاندازی کنیم.

معاون پرورشی و فرهنگی وزارت آموزش و پرورش درباره اقدامات آموزش و پرورش در زمینه مبارزه با آسیب‌های فضای مجازی اظهار کرد: سیاست آموزش و پرورش سیاست مقابله و فرار نیست، بلکه حضور و مشارکت فعال در این عرصه را مدنظر داریم.

کفاش ادامه داد: برای جلوگیری از آسیب‌ها اولین راهکار آموزش است. در سطح کشوری، استانی، منطقه‌ای و مدرسه آموزش‌های لازم به دانش آموزان ارائه می‌شود. دانش آموزان باید استفاده صحیح از فضای مجازی را بیاموزند و از مخاطرات آن آگاه باشند.

وی با بیان اینکه آموزش به خانواده‌ها نیز حائز اهمیت است عنوان کرد: آموزش به خانواده دانش آموزان توسط انجمن اولیا و مربیان ساماندهی می‌شود و در جلسات مختلف تهدیدها و فرصت‌های فناوری را تشریح می‌کنند تا والدین بدانند چگونه باید از فرزندشان در مقابل این تهدیدات محافظت کنند.

معاون پرورشی و فرهنگی وزارت آموزش و پرورش افزود: بعد دیگر نیز آموزش و آگاه‌سازی معلمان است. ما سعی می‌کنیم دانش آموزان را با ابعاد مثبت فضای مجازی آشنا و به وبلاگ نویسی، ایجاد نشریات الکترونیکی و حضور فعال در فضای مجازی تشویق کنیم.

پیاده تا بهشت



اینفوگرافیک | ۷

توصیه امنیتی به والدین در خصوص استفاده نوجوانان از تلفن‌های همراه

امروزه استفاده از تلفن همراه در بین کودکان در حال افزایش می‌باشد. 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.

اجتماعی | ۵

مهارت‌های امنیتی کار با تلفن همراه

در فضای جامعه پیشرفته امروزی تلفن همراه به یکی از لوازم ضروری زندگی تبدیل شده است. در این زمان کمتر کسی را می‌توان پیدا کرد که حداقل یک خط به همراه یک گوشی تلفن همراه نداشته باشد.

گوشی‌های هوشمند | ۲

مهارت‌های امنیتی کار با تلفن همراه



در فضای جامعه پیشرفته امروزی تلفن همراه به یکی از لوازم ضروری زندگی تبدیل شده است. در این زمان کمتر کسی را می‌توان پیدا کرد که حداقل یک خط به همراه یک گوشی تلفن همراه نداشته باشد. در واقع تلفن همراه به یک دفتر کار و بانک اطلاعات تبدیل شده است و اطلاعات مهمی نظیر، پیامک‌های خصوصی، نشانی و شماره تلفن افراد مختلف، شماره حساب‌های بانکی و رمز آن‌ها، عکس‌های خانوادگی و موارد بسیار دیگری در آن ذخیره شده است.

صاحب تلفن همراه برای حفاظت از این اطلاعات مهم باید نکات مهم امنیتی را رعایت کند که در ادامه به برخی این نکات اشاره می‌شود:

۱. داشتن شماره سریال و کد حذف اطلاعات

هر گوشی تلفن همراه دارای یک شماره سریال مخصوص به خود است. این شماره به شخص کمک می‌کند تا علاوه بر این که با مراجعه به سایت اصلی شرکت تولید کننده گوشی همراه، از اصل بودن آن مطمئن شود. در صورت مفقود یا ربوده شدن گوشی، از طریق مراجع قضایی نسبت به یافتن آن اقدام کنید. یکی از راه‌ها برای بدست آوردن شماره سریال تلفن همراه برای برخی گوشی‌ها این است که کلیدهای *#۶۰# را به ترتیب وارد کرده و بعد کلید سبز یا تماس را فشار دهید. این شماره مختص به دستگاه شماست. در مواقعی که تلفن همراه شما به سرقت می‌رود شما می‌توانید با پشتیبان شبکه خود تماس گرفته و این کد را به آن‌ها بدهید. سپس آن‌ها قادر خواهند بود تلفن همراه شما را مسدود کنند. امکان دارد شخص دیگر نتواند تلفن خود را پس بگیرد ولی این تلفن همراه دیگر کارایی ندارد و شخص دیگری حتی اگر سیم کارت آن را عوض کند، قادر به استفاده از آن نیست.

۲. موقعیت مکانی

برخی تلفن‌های همراه به گونه‌ای طراحی شده‌اند که برخی از اجزای آن‌ها به صورت خودکار شرکت خدمات دهنده تلفن همراه از مکان فعلی شما با خبر می‌کنند. افزون بر این مورد بعضی از تلفن‌های همراه مجهز به سیستم GPS هستند و این اطلاعات دقیق ممکن است در داده‌های دیگری در عکس‌ها، پیامک و جست و جوی اینترنتی که از طریق تلفن همراه انجام می‌شوند، جا سازی شده باشند.

۳. رمز گذاری گوشی و سیم کارت

اکثر تلفن همراهی که در بازار وجود دارند در قسمت تنظیماتشان برای محافظت از آن چه در گوشی و حافظه آن ثبت شده است گزینه‌ای برای تعیین کلمه عبور وجود دارد. شخص با رمز گذاری تلفن همراه خود در واقع دسترسی برای افراد دیگر را غیر ممکن می‌کنند این رمز گذاری می‌تواند به صورت عدد، کلمه و یا ترکیبی از این دو یا حتی تصویری نیز باشد. همچنین برای سیم



کارت‌هایی که در بازار هستند امکان رمز گذاری وجود دارد. در قسمت تنظیمات تلفن همراه با فعال کردن قفل سیم کارت یا پین کد می توان مانع از به کارگیری دستگاه توسط اشخاص دیگر شد .

۴. ناامن ترین پروتکل

یکی از امکانات جانبی اکثر تلفن‌های همراه بلوتوث است؛ ولی بلوتوث یکی از ناامن ترین پروتکل‌های ارتباطی در دنیاست. در واقع مزیت بلوتوث این است که به راحتی می توان بدون سیم به گوشی دیگر متصل شده و اطلاعات را منتقل کرد و اگر کاربر از نحوه کارکرد آن مطلع باشد می تواند از امکانات آن استفاده کند. این فناوری در شعاع ۱۰ متری اطلاعات را در هر دستگاهی مانند تلفن همراه و لپ تاب و تبلت منتقل می کند. در عین حال ممکن است ارتباط بلوتوث شما هک شود؛ یعنی هنگامی که بلوتوث شما روشن است و در حال انتقال اطلاعات هستید هکر از این فرصت استفاده کرده و به راحتی به تلفن همراه شما دسترسی پیدا می کند. این حالت حتی برای زمانی که بلوتوث روشن است و از آن استفاده نمی کنید؛ نیز قابل تصویر است.

بنابراین توصیه می شود که هنگامی که از بلوتوث استفاده نمی کنید یا زمانی که در حال مکالمه هستید یا اطلاعات شخص را وارد تلفن همراه می کنید بلوتوث را در حالت خاموش قرار دهید و اگر می خواهید از بلوتوث استفاده کنید اتصال خود با گوشی دیگر را با یک رمز طولانی و امن تر برقرار کنید.

۵. رمز گذاری برای اطلاعات مهم

معمولاً تلفن‌های همراه می توانند اطلاعات مهمی را در حافظه خود ذخیره کنند. این اطلاعات می تواند شامل عکس‌ها، کلیپ‌های ویدئویی، فایل‌های متنی، سابقه تماس‌های تلفنی، اطلاعات افراد ذخیره شده در لیست تلفن و اطلاعات شخص صاحب گوشی تلفن همراه باشد. محافظت از این اطلاعات مشکل و در عین حال مهم و ضروری است. از این رو انتخاب گوشی تلفن همراه دارای اهمیت ویژه‌ای می باشد؛ بنابراین سعی کنید گوشی تلفنی را انتخاب نمایید که دارای قابلیت رمز گذاری برای بخش‌های مختلف اطلاعات باشد.

۶. داشتن نسخه پشتیبان

فناوری‌های نوین با وجود داشتن مزیت‌های بی شمار، همیشه قابل اطمینان نیستند؛ شاید برای شما هم این موضوع اتفاق افتاده باشد که تمام اطلاعات ذخیره شده بر روی تلفن همراه خود را به دلایل مختلف اعم از گم شدن تلفن یا خراب شدن آن از دست داده باشید. معمولاً کاربر حرفه‌ای از تمامی اطلاعات تلفن همراه خود یک نسخه پشتیبان دارد انواع نرم افزارهای گرفتن بک آپ یا نسخه پشتیبان در اینترنت وجود دارد. همچنین بعضی از شرکت‌های تلفن همراه برای گرفتن نسخه پشتیبان اطلاعات نرم افزاری را در سایت‌شان جهت دانلود قرار می دهند.

توصیه امنیتی به والدین در خصوص استفاده کودکان از تلفن‌های همراه



امروزه استفاده از تلفن همراه در بین کودکان در حال افزایش می باشد. 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. هر زمان که فرزندان برای استفاده از تلفن هوشمند آماده بودند، به آنها در خصوص ایمنی و مسئولیت پذیری آموزش های لازم را بدهید.

در این مقاله به موارد زیر پرداخته می شود:

- تلفن‌ها، قابلیت‌ها و گزینه‌ها
- به اشتراک گذاری و شبکه سیار
- برنامه‌های کاربردی تلفن همراه
- پیام رسانی

• تلفن‌ها، قابلیت‌ها و گزینه‌ها

درباره گزینه‌ها و قابلیت‌های مناسب تصمیم گیری کنید

تلفن همراه و شرکت‌های تلفن سیار (wireless company) معمولاً 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.



تلفن‌های محافظت شده با کلمه عبور

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

• به اشتراک گذاری و شبکه سیار

به اشتراک گذاری و اجتماعی بودن می‌تواند فرصت‌ها و چالش‌هایی 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 گردد.

هنگام به اشتراک گذاری تصاویر و ویدئوها مراقب باشید

بیشتر تلفن‌های همراه قابلیت عکس گرفتن و تصویربرداری را دارند و به اشتراک گذاری و گرفتن تصاویر را در هر لحظه آسان می‌کنند. فرزندان 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 بعداً بخواهیم خسارت را کنترل کنیم ساده‌تر است.

• برنامه‌های کاربردی تلفن همراه

درباره برنامه‌های کاربردی چه باید بدانیم؟

برنامه‌های کاربردی ممکن است:

- اطلاعات شخصی را جمع‌آوری و به اشتراک بگذارند
- رایگان باشند اما فرزندان شما را ترغیب به پرداخت پول کنند
- شامل تبلیغات باشند
- به رسانه‌های اجتماعی (social media) متصل باشند.

اما برنامه‌های کاربردی ممکن است به شما درباره کارهایی که انجام می‌دهند چیزی نگویند.



چه کار می توان انجام داد؟

کارهایی وجود دارند که شما و فرزندتان می توانید قبل از دانلود برنامه برای یادگیری درباره برنامه های کاربردی انجام دهید:

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

آیا می توانیم چگونگی استفاده از برنامه های کاربردی توسط کودکان را محدود کنیم؟

قبل از اینکه تلفن یا تبلت خود را به فرزندتان بدهید، به تنظیمات آن نگاه کنید. ممکن است قادر به انجام کارهای زیر باشید:

- 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.
- خدمات داده و وای فای را خاموش کنید تا به اینترنت متصل نشوید. همچنین می توانید تلفن را در حالت پرواز قرار دهید.
- بهترین راه برای مراقبت در قبال برنامه های کاربردی کودکان تست و بررسی توسط والدین است. با فرزندتان خود درباره قوانین خرید و استفاده از برنامه های کاربردی صحبت کنید.

• پیام رسانی

از حریم خصوصی محافظت کنید

به کودکان خود یادآوری کنید که:

- متن هایی 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

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.
 - ❖ می توانند منجر به شارژ هزینه های ناخواسته در صورت حساب تلفن همراه شما شوند
 - ❖ می توانند کارایی تلفن همراه شما را پایین بیاورند.

چه کار می توان انجام داد؟

- صورت حساب تلفن همراه خود را بررسی کنید و ببینید آیا هزینه های غیرمجازی در صورت حساب خود مشاهده می کنید؟ به فرزندان خود بگویید:
- ❖ پیام هایی را که اطلاعات شخصی را درخواست می کند حذف کنید؛ حتی اگر وعده هدیه رایگان را می دهد. شرکت های قانونی اطلاعاتی مانند شماره حساب ها یا کلمات عبور را از طریق ایمیل یا متن درخواست نمی کنند.
 - ❖ 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.

راهنمای کامل عزاداران حسینی در راهیمای عظیم اربعین

پیاده تابهشت

علامت های مومن (شیعه) پنج چیز است: خواندن پنجاه و یک رکعت نماز در شبانه روز، زیارت اربعین، انگشتر به دست راست کردن پیشانی را در سجده بر خاک نهادن و بلند گفتن بسم الله الرحمن الرحیم در نماز امام حسن عسکری (ع)

هر کس با ترس به زیارت قبر حسین (ع) بیاید، خداوند او را از ترس و وحشت، در روزی که مردم برای پس دادن حساب به خداوند جهانیان برمی خیزند، در امان نگه امام صادق (ع) دارد.

کسی که از منزلش بیرون آید و قصدش زیارت قبر حضرت حسین این علی (ع) باشد، خداوند نشان به هر قدمی که برمی دارد یک حسنه برایش نوشته و یک گناه از او محو می فرماید. امام صادق (ع)

لوقطعوارجلناولیدین ناتیکنزحفا سیدی یا حسین (ع)

اگر دست و پاهایمان را هم قطع کنند به زیارت نومی آیم یا حسین (ع)



۵ برای پیاده روی گوله بستی سبک انتخاب کنید، وسایلی کم وزنی همراه داشته باشید.

۲ برای درمان بیماری های خفیف مقداری آنتی بیوتیک همراه خود داشته باشید.

۴ لباس های مناسب: جوراب، دستکش، کلاه، پوشش گوش، کاپشن و کفش مناسب...

۲ قرآن، دعا و زیارت جیبی با نرم افزار های مذهبی موبایلی جهت مناجات همراه داشته باشید.

۱ پاسپورت و شارژ موبایل گرم مناسب برای تاول و عرق سوز همراه داشته باشید.

۱ مراکز افراد گمشده در ستون های ۱۱۰۳۰۶۰۲۳۵۷۲ و حرم حضرت عباس قرار دارند.

۳ سرویس بهداشتی و همچنین پل های شارژ موبایل در سراسر مسیر موجود است.

۵ بهتر است زائران، پیاده روی را از طلوع آفتاب آغاز و در مغرب توقف کنید.

۴ به دلیل ترافیک بالای شبکه در روز، مکالمات تلفنی را قبل از طلوع آفتاب انجام دهید.

۲ برای زائران کم توان صدها، ماشین و یا نوبس برای رسیدن به کرپلادر مسیر وجود دارد.

- ۱ موبایل
- ۲ تلفن
- ۳ دارو
- ۴ کلاه
- ۵ کفش

- ۱ آفتاب
- ۲ اتوبوس
- ۳ عینک
- ۴ دوربین
- ۵ هدفون

بیشتر بدانیم

تعداد ستون های مسیر ۱۴۵۲ عدد

میزان مسافت از نجف ۸۰ کیلومتر

فصل بهار ۵۵ متر

زمان پیاده روی ۲۵ ساعت

