Family Safety on The Internet

چگونه امنیت خانواده مان را در اینترنت حفظ کنیم؟

چگونه با خردسالان، کودکان و نوجوانان و هر شخص تازه‌کار در مورد امنیت آنلاین سخن بگویید

گردآوری و تنظیم کننده : رضا فریدون نژاد

سلام ؛

کتاب شماره ۱۶ از **مجموعه دانش و زندگی** ، با عنوان چگونه امنیت خانواده را در اینترنت حفظ کنیم ؟ تقدیم به شما خواننده محترم.امیدوارم این کتاب مورد استفاده شما قرار بگیرد.

" کتابهای الکترونیکی دانش و زندگی را به دوستانتان معرفی کنید "

" کاربر محترم ، هر زمان که کتابهای دانش و زندگی را دانلود و مطالعه نمودید نظر خود را درباره همان کتاب و یا دیگر کتابها به من اعلام نمایید (از نظر مفید بودن مطالب ارائه شده،موضوعات انتخاب شده،داشتن طراحی جلد مناسب،روان و قابل فهم بودن متن کتاب و ...) ، **منتظر نظرات ، پیشنهادات و انتقادات سازنده شما عزیزان هستم"**

نظر شما در مورد این کتاب و دیگر کتابهای ارائه شده چیست؟

www.dzbook.ir

rezaf1390@gmail.com

با آرزوی موفقیت و سلامتی برای شما

رضا فریدون نژاد

مقدمه

میلیون‌ها خانواده در سرتاسر دنیا هر روز از اینترنت برای یادگیری، پژوهش، خرید و فروش، استفاده از خدمات بانکی، سرمایه‌گذاری، به اشتراک گذاری عکس، بازی کردن، دانلود فیلم و موزیک، ارتباط با دوستان، آشنا شدن با افراد جدید و مشارکت در میزبانی برای سایر فعّالیّت‌ها استفاده می‌کنند. گرچه فضای مجازی مزایا، فرصت‌ها و آسودگی‌های متعدّدی را به ارمغان می‌آورد، امّا به صورت افزایشی خطرناک است به طوری که روزانه بسیاری از تهدیدهای جدید ظهور و بروز می‌یابند.

جای تعجّب نیست که مجرمان اینترنتی به دنبال استفاده از اینترنت و کسانی هستند که آن را به کار می‌برند. شما و اعضای خانواده‌ی شما نیاز دارید که هر زمان که آنلاین می‌شوید در امنیت باشید.

علاوه بر نصب نرم‌افزارهای امنیتی قوی از محصولات شرکت‌های قابل اعتماد برای دفاع از خانواده‌ی خود در برابر هکرها، سارقان هویّت، کلاهبرداران ایمیلی و تبه‌کاران، شما باید برخی از قوانین ابتدایی ایمنی در اینترنت را نیز دنبال کنید و از قدرت تعقّل خود استفاده کنید. شما به یک برنامه‌ی امنیت اینترنتی برای خانواده‌ی خود نیاز دارید.

به محض آن که یکی از اعضای خانواده، فعّالیّت‌های آنلاین خود را آغاز می‌کند، فارغ از آن که در چه سنّ و سالی هستند، زمان آموزش وی درباره‌ی امنیت سایبری فرا می‌رسد. شما باید آگاه باشید که اگر حتّی در خانه کامپیوتر ندارید، کامپیوترهای شخصی تقریباً در هر جایی هستند. در مدارس، کتابخانه‌ها، خانه‌ی دوستان، حتّی در زیرزمین کلیسا (در مسجد). این که هر کسی دانش ابتدایی حفاظت از خود در فضای سایبری را بداند، بسیار مهم است.

والدین در دنیای آنلاین

اگر به عنوان پدر یا مادر در آخرین تغییرات اینترنت یا وب سایت های محبوب با فرزندانتان همگام نباشید مسئله ای نیست. لازم نیست برای اینکه به فرزندانتان کمک کنید از اینترنت لذت ببرند با همان سرعتی که همه چیز پیش می رود پیش روید. آنچه ابتدا باید انجام دهید این است که راجع به آنچه فرزندتان در وب انجام می دهد با وی صحبت کنید، سپس برای خانواده خود قوانین را توضیح داده و آنقدر این صحبت ها را هر سال ادامه دهید تا به قدر کافی بزرگ شده و بتوانند مواظب خود باشند.

قبل از صحبت با فرزندانتان مهم است نحوه درک و پاسخ خود را زمانی که صحبت از زندگی دیجیتال آنها به میان می آید و موضوعاتی که با آنها روبرو هستند تحلیل نمایید. در اینجا آمارهایی وجود دارد که در این زمینه می تواند مفید باشد:

- کودکان از نظر شخصیتی احساس مسئولیت می کنند: بیش از ۷۷٪کودکان از اینکه یک ویروس را دانلود کرده بودند احساس مسئولیت می کردند و نزدیک به ۶۳٪ به خاطر پاسخ دادن به یک کلاهبرداری اینترنتی احساس گناه می نمودند.
- بیش از ۵۳٪ کودکان فیلم و موسیقی دانلود می کنند ولی تنها ۳۸٪ والدین از این موضوع اطلاع دارند.
- اکثر والدین در منازل خود برای استفاده از اینترنت قانون دارند ولی تنها ۳۷٪ آنها کنترل های والدینی را روی کامپیوترهایشان تنظیم کرده اند.

از فرزندان خود محافظت کنید

در اینجا چند گام ارائه شده است که به کمک آنها خانواده ها می توانند از کودکان خود در برابر خطر اینترنت و تکنولوژی کامپیوتر محافظت کنند. ابتدا والدین باید این نکته را در نظر داشته باشند که نظارت و توصیه های بزرگتران ضروری است و نه اختیاری. همان طور که به کودکان آموخته می شود چگونه باید از خیابان عبور کنند باید آنچه را که در وب انجام می دهند را نیز مورد نظارت قرار داد. ابتدا با کودکان خود دراین باره صحبت و گفتگو کنید که چه وقت و چه مدت می توانند در اینترنت بمانند و از چه سایت هایی مجازند که دیدن کنند. سایت های محبوب آنها را bookmark کنید تا دسترسی راحت تری داشته باشند. هنگامی که کودک از کامپیوتر استفاده می کند او را تنها نگذارید، یا کامپیوتر را در اتاقی بگذارید که معمولا اعضای خانواده در آن حضور دارند.

کامپیوترها در حال تغییر نحوه تعامل انسان با دیگران و دانش اندوزی وی از دنیای اطرافش هستند و نقش بسیار مهمی در زندگی روزانه انسان ایفا می کنند . نمی توان تظاهر کرد که این تغییرات اتفاق نمی افتند. با پذیرفتن مسئولیت استفاده کودکان از کامپیوتر، خانواده ها می توانند به شدت خطرات و تهدیدات را

کاهش دهند و در عین حال به کودکانشان اجازه دهند تجربیات مثبت و بسیار مفیدی بدست آورند.

استفاده روزافزون از کامپیوترها نیازمند نظارت بهتر است.

هر یک از پنج کودک در دنیا می پذیرند که در اینترنت کارهایی را انجام می دهند که والدینشان به آنها اجازه نمی دهند. در حالی که نیمی از والدین می گویند که درباره امنیت در اینترنت با کودکانشان صحبت می کنند، با این وجود این کار را تنها یکبار و بصورت دو نصیحت انجام می دهند: مردم در دنیای آنلاین معمولا همان که تظاهر می کنند نیستند" و "در دینای آنلاین از غریبه ها حذر کنید". تعجبی ندارد که در این صورت کودکان می ترسند به شما بگویند اشتباهی در اینترنت مرتکب شده اند که مبادا شما کامپیوتر آنها، ارتباط آنها با اینترنت، تماس آنها با دوستانشان و بقیه جهان را نگیرید. هنگامی که صحبت از دنیای آنلاین است کودکان می اندیشند که پدر و مادر ها چیزی را درک نمی کنند.

آنچه در آغاز کار نیاز دارید

در صورتی که مایل بودید با کودکانتان صحبت کرده و بدانید که در اینترنت چه کاری انجام می دهند می توانید با این سوالات شروع نمایید:

۱- دوستانتان در اینترنت چه کار می کنند؟

این سوال توجه را از کودک منحرف کرده و به فعالیت های اینترنتی عمومی در اطراف وی هدایت می کند. این روش خوبی برای آغاز کار و ساده و عادی نگاه داشتن موضوع است. شما باید کودکانتان را مطمئن سازید که به خاطر پاسخ هایشان آنها را تنبیه نخواهید کرد. با این روش می توانید اطلاعاتی درباره بازی، چت، شبکه های اجتماعی و حتی تکالیف و فعالیت های تحقیقاتی آنها کسب کنید.

۲- جدیدترین و پرطرفدارترین وب سایتها کدامند؟

از کودکان خود بپرسید این سایت ها چرا محبوبیت دارند. همچنین می توانید درباره سایت هایی که محبوبیت ندارند نیز بپرسید.

۳- سایت های مورد علاقه خود را به من نشان بده

بله، بهتر است اندکی از زمان خود را صرف این کنید که سایت های مورد علاقه کودکان را تماشا کنید. از آنها بپرسید تنظیمات امنیتی خود را چگونه انجام می دهند (به بالا و پایین صفحات آن سایت ها دقت کنید). در صورتی که تصمیم می گیرید خودتان این تنظیمات را برقرار کنید اجازه دهید کودکان نیز در جریان کار قرار گیرند.

۴- آیا تاکنون زمانی که آنلاین بودید با مورد عجیبی برخورد کرده اید یا احساس ناراحتی نموده اید؟

در اینجا می توانید در مورد جستجوهای تصادفی کودکانتان در وب سوال کنید .ایده این روش این است که مطمئن شوید کودکانتان بدانند می توانند صحبت کنند و اگر اتفاق بدی در دنیای آنلاین بیافتد تنبیه نخواهند شد. به هر حال تجربه های ناخوشایند، در صورتی که کودکتان عضو فعالی در وب باشد، اجتناب ناپذیر است. بگذارید فرزندتان بداند که اگر اتفاق بدی افتاد می تواند جهت کمک به شما مراجعه کند و تنبیه نخواهد شد.

با وجود اینکه بازی یکی از محبوب ترین سرگرمی های کودکان است، بازی آنلاین همیشه یک تفریح نیست. به طور متوسط ۶۲ در صد کودکان در سراسر دنیا، تجربه ای ناخوشایند آنلاینی در این زمینه داشته اند. تنها ۴۵ درصد والدین می اندیشند که کودکان آنها ممکن است از تجربیات منفی در دنیای آنلاین رنج ببرند. خبر خوب این است که اگر اتفاق بدی در اینترنت برای کودکان بیافتد برای مشورت و کمک خواستن نزد والدینشان می روند. آمار نشان می دهد که:

۸۷٪ در صد کودکان اگر تهدید به آسیب فیزیکی شوند به والدینشان اطلاع می دهند

۸۴٪ درصد آنها در صورتی که blackmail دریافت کنند به والدین خود خواهند گفت

۷۱٪ درصد آنها مسائل مشکوک و نامناسب را گزارش می دهند

محتویات دانلود

بیش از ۵۱ درصد کودکان می گویند که والدینشان به آنها اجازه می دهند بدون هیچ نظارتی، بازی ها را روی کامپیوتر خود دانلود کنند. والدین باید خطر دانلودهای رایگان را در کامپیوتر خود از بین ببرند. بدون بروزرسانی کردن سیستم های امنیتی و آنتی ویروس روی سیستم، کامپیوتر براحتی با برنامه های مضر آلوده می شود. کودکان نیز ممکن است قربانی قراردادهای ناخواسته و پرداخت های وجه ناآگاهانه شوند. مثلا ممکن است به جای شارژ حساب بانکی و کارت اعتباری شماره موبایل را وارد کرده و آن را شارژ کنند.

علاوه بر قوانین والدین، ۹۵ درصد کودکان قوانین خود را نیز در دنیای آنلاین دارند. در حالی که والدین بر محدودیت زمانی در استفاده از اینترنت و کاهش

میزان جستجوها تاکید می کنند کودکان بر روش رفتار تاکید و توجه دارند.

ابزارهای کنترل والدین پیشرفته

در کنار انتخاب دقیق شما در رابطه با تنظیمات صحیح امنیتی، می توانید از مزایای برخی ابزارهای کنترلی والدین که در مجموعه آنتی ویروس های معروف عرضه می گردند نیز استفاده نمایید و مثلا می توانید سایت هایی را که کوکانتان مشاهده می کنند بررسی کرده و ببینید که موارد مضر و نامناسبی دارند یا خیر. علاوه بر آن می توانید زمانی را که در برخی از سایت ها می گذرانند را نیز مشاهده کنید این کار در تنظیم زمان فرزندتان برای انجام تکالیف مدرسه و کار با اینترنت کمک میکند. بدین وسیله می توانید هر زمان که لازم بود کامپیوتر را خاموش کنید تا مطمئن شوید که قوانین اجرا می شوند.

فرزندان در چه سنی از کامپیوتر و اینترنت استفاده کنند؟

استفاده از کامپیوتر و اینترنت برای کودک و نوجوان باید به طور کلی مترادف با مسئولیت پذیری، قانونمندی و طبعا محدودیت باشد، والدین باید ضمن تفهیم این اصول، به فرزندان خود یاد بدهند که اجازه چه فعالیت هایی را با کامپیوتر و اینترنت دارند، از چه فعالیت هایی باید به دور باشند.

نرم افزارهای آموزشی و بازی های بسیار ساده ای وجود دارد که با توجه به تصاویر، رنگ و موسیقی برای کودکان از حدود سه سالگی جذابیت دارد. از حدود ۴ سالگی تا شروع مدرسه، میل، و ولع به یادگیری کار با کامپیوتر و بازی در کودکان زیاد می شود.

در همین سنین درباره اصول استفاده از اینترنت و کامپیوتر برای بچه ها مقدمه چینی و صحبت کنیم و اما برای بچه های دبستانی باید قوانین مشخص و محکمی جهت استفاده از اینترنت تعریف، تفهیم و اجرا شود و عوارض عدم رعایت قوانین نیز به آنها گوشزد شود.

با ورود به نوجوانی جنگ و جدال های استقلال طلبانه فرزندان با والدین بر سر موضوعات مختلف شروع می شود که یکی از این موضوعات درخواست استفاده آزادانه، دلخواه و بدون نظارت از اینترنت است. این سن، سن هشدار است و ضمن مذاکره و توافق با فرزندان، اصول توافقی بسیار روشن و صریح باید اجرا شود. فرزندان تحت نظارت کامل می توانند به تحقیق و فعالیت اینترنتی محدود و مشخص چه از نظر حجم ساعات مورد استفاده و چه موضوع مورد استفاده بپردازد.

به طور کلی استفاده از کامپیوتر و اینترنت برای کودک و نوجوان مترادف با مسئولیت پذیری، قانونمندی و طبعا محدودیت است. والدین باید ضمن تفهیم این اصل، به او یاد بدهند که اجازه چه فعالیت هایی را با کامپیوتر و اینترنت دارد، از چه فعالیت هایی باید به دور باشد و چگونه با پیام ها و موضوعاتی که در اینترنت او را ناراحت می کند برخورد صحیح کند.

تامین امنیت فرزندان هنگام استفاده از کامپیوتر و اینترنت

در اینجا یک راهنمای ساده و کاربردی تهیه کرده ایم که چگونه کامپیوتر خانه را به ابزاری امن و محلی برای پرورش خلاقیت کودکان پیش دبستانی تا نوجوانان تبدیل کنیم.

تامین امنیت کودکان هنگام استفاده از کامپیوتر و اینترنت، مطمئنا در سنین مختلف، ابزارها و شیوه های متفاوتی را نیاز دارد و روش برخورد از یک کودک ۲ ساله تا یک نوجوان کاملا فرق می کند.

برای تمام سنین

سیستم عامل های ویندوز شرکت مایکروسافت امکانات کنترلی رایگانی را بر روی خود دارند که به والدین اجازه می دهد تا سایت های با محتوای ویژه بزرگسالان، دانلودها و سایت های مشخصی را بر روی کامپیوتر مسدود کنند. حتی در خصوص بازی ها هم می توانید بازی های با رده بندی ویژه ای را که

مناسب کودک شما نیست، ببندید. حتی محدودیت های تان را می توانید به ساعات و روزهای خاصی از هفته محدود کنید. تنظیمات ویژه والدین را می توانید در آدرس زیر بیابید:

Start > Control Panel > User Accounts >Set up Parental Controls

یک امکان دیگر، استفاده از تنظیمات موتور جستجوهای مختلف برای محدود کردن و کنترل نتایج جستجو است. مثلا موتورهای جستجو بینگ یا گوگل این قابلیت را دارند که در نتایج جستجوی شان محتوای ویژه بزرگسالان را به نمایش نگذارند.

تمام تنظیمات مورد نظر بر روی ویندوز، با یک رمزعبور ویژه والدین حفاظت می شوند که در اختیار هیچ یک از کودکان قرار نمی گیرد. والدین حتی می توانند تنظیمات لازم را برای اکانت های مختلف جهت فرزندان سنین متفاوت انجام دهند و به هر کدام نام کاربری و رمزعبور جداگانه ای اختصاص دهند. با این اکانت فرزندان می توانند از کامپیوتر استفاده کنند، اما قادر به تغییر تنظیمات والدین نخواهند بود.

با همه این حرف ها، آکادمی متخصصین کودک آمریکا در گزارش مارس ۲۰۱۱ خود با عنوان «اثر رسانه های اجتماعی بر کودکان، نوجوانان و خانواده» اخطار کرده اند که اینگونه راه حل ها و کنترل های تکنیکی به تنهایی راه گشا نیستند. مشارکت فعال و ارتباط موثر والدین با کودکان هم بسیار مهم است.

یک طرح برای فعالیت های آنلاین خانواده پایه گذاری کنید که شامل جلسات خانوادگی منظمی باشد و در آنها درباره موضوعات مربوط به فعالیت های آنلاین و شیوه و تنظیمات کنترل حریم خصوصی بحث و تبادل نظر کنید. در این جلسات همچنین شیوه برخورد با افراد سودجو و پیام های بی مورد را به فرزندان و اعضای خانواده بیاموزید. در این جلسات دوره ای باید تاکید بر عادات کاربری سالم و اخلاق نت وندی بوده و رفتارهای تنبیهی پیش بینی نشود.

قبل از مدرسه ۲ تا ۴ سال: بازی در چاله شنی

در حالی که هنوز سن مناسب برای شروع کار کودک با کامپیوتر جز مناظرات و بحث های داغ مجامع علمی است، اما واقعیت این است که بچه ها دوست دارند کاری را که مامان شان انجام می دهد، تکرار کرده و انجام دهند. کار با کامپیوتر هم از این قاعده مستثنی نیست.

سگال دروری متخصص پیشرفت کودکان در کالج آموزشی لوینسکی می گوید: «والدین باید به خاطر داشته باشند که کامپیوتر یک ابزار کمک آموزشی است که فرزند آنها را برای رویارویی با دنیا آماده می کند. کودکان با کامپیوترها به دنیا می آیند و هر روز والدین شان را در حال کار با کامپیوتر می بینند. پس این کاملا عادی است که آنها به کامپیوتر به عنوان یک محیط بازی و سرگرمی نگاه کنند».

برای کودکان پیش از مدرسه، والدین می توانند محیط بازی ویژه کودک را ایجاد کنند. ایجاد یک فضای کاملا محافظت شده به همراه دسترسی به اینترنت جهت آموزش های اولیه و سرگرمی های کودکانه گزینه مناسبی به نظر می رسد. اگر چه سایت مناسب آموزشی-سرگرمی به زبان فارسی نداریم، اما با کمی جستجو می توانید سایت های انگلیسی زبانی چون Kneeboucers.com را بیابید که تا حدی قابل استفاده اند.

یک انتخاب مناسب دیگر به زبان انگلیسی، می تواند برنامه Zoodles باشد که حاوی بازیها و فعالیت هایی برای کودکان پیش دبستانی است. این برنامه به والدین اجازه می دهد سطح و توانایی مورد نظر را که می خواهند کودکان شان یاد بگیرند، انتخاب کنند. این برنامه هنگام اجرا، تمام صفحه کامپیوتر را در اختیار می گیرد و به کودکان اجازه کار دیگری با سیستم را نمی دهد.

سالهای اولیه مدرسه، سنین ۵ تا ۷ سال: اینترنت با چرخ های کمکی

به محض اینکه کودکان خواندن و نوشتن را یاد بگیرند، آماده دستیابی به تجربیات اینترنتی بیشتری همچون جستجو، بازی و سرگرمی هستند. استفاده از مرورگرهای ویژه کودکان، برای این سنین مناسب به نظر می رسند.

برای مثال برنامه KidZui یک رابط کاربری آسان برای دست یابی به میلیونها وب سایتی است که برای کودکان طراحی شده اند. در این مرورگر، کودکان توانایی بوک مارک کردن و جستجوی صحیح را می آموزند و به گشت و گذار در دنیای وب می پردازند.

این برنامه می تواند دسترسی محدود به بسیاری از سایت ها همانند یوتیوب را مهیا کند. در این حالت تنها برخی ویدیوهای مورد نظر والدین در دسترس کودک قرار می گیرند، امکان چت در همه سایت ها و برنامه ها بسته می شود و می توان آن را به گونه ای تنظیم کرد که با روشن شدن سیستم فعال شود و برای خروج از آن و استفاده عادی از سیستم، باید رمزعبور را وارد کرد.

سالهای میانی مدرسه، سنین ۸ تا ۱۲ سال: اجتماعی شدن

جذابیت شبکه های اجتماعی ممکن است از کلاس سوم، چهارم یا پنجم شروع شود. اما متخصصان کودکان اخطار می کنند که پریدن در گرداب شبکه های اجتماعی، با توجه به تاثیر کودکان بزرگتر در این سن، ممکن است بسیار زودهنگام باشد.

فیس بوک اطلاعات کودکان زیر ۱۳ سال را نمی پذیرد و به آنها اجازه عضویت نمی دهد. در صورتی هم که پروفایل کودکان زیر ۱۳ سال را که با تاریخ تولد جعلی عضو شده اند پیدا کند، سریعا انها را پاک می کند. این سن بر اساس قوانین آمریکا برای حمایت از حریم خصوصی آنلاین کودکان تعیین شده است. این قانون وب سایت ها را از جمع آوری و ثبت اطلاعات کودکان زیر ۱۳ سال بدون اجازه والدین منع می کند.

اما جالب است بدانید که طبق آمار تقریبی کاربران، بیش از ۷.۵ میلیون کاربر زیر ۱۳ سال در فیس بوک عضو هستند.

نوجوانان، ۱۳ سال به بالا: رقابت در فیس بوک

در سالهای نوجوانی دوستان و روابط اجتماعی از اهمیت بالایی برخوردار هستند. طبق یک تحقیق در سان فرانسیسکو، بیش از نیمی از افراد این گروه سنی، بیش از روزی یک بار به شبکه های اجتماعی سر می زنند. ۲۲ درصد از نوجوانان، روزانه بیش از ۱۰ بار این کار را انجام می دهند.

برخی از جوانان وسوسه شبکه های اجتماعی را چنان سخت می یابند که توان مقاومت در برابر آن را ندارند. تا جایی که فعالیت در شبکه های اجتماعی با انجام تکالیف، خواب و فعالیت های فیزیکی آنها تداخل پیدا می کند.

عکس ها می توانند کپی شده، پیست شده، اسکن شده، ایمیل شده و به هرجایی بروند. کسی چه می داند که وقتی ۲۰ ساله شوید، عکس های میهمانی دوران دبیرستان تان از کجا سر در آورده اند؟! اینکه چیزی را برای اولین بار در جایی کپی نکنیم، بسیار ساده تر از این است که در آینده تمام تلاش تان را برای حذف و پاک سازی آن از دنیای اینترنت به هدر دهیم.

چه باید کرد؟ با نوجوان تان به بررسی تنظیمات امنیتی و حریم خصوصی اکانت فیس بوک وی بپردازید. تنظیمات پروفایل وی حتما باید در حالت خصوصی (Private)باشد. همچنین اطمینان یابید که او می داند انتشار عکس های خصوصی اش در اینترنت، مشکلات فراوانی در آینده ایجاد خواهد کرد. فرزند شما نباید هیچ درخواست دوستی از طرف افراد ناشناس را بدون اطلاع شما قبول کند. اگر والدین هم عضو فیس بوک هستند، حتما فرزندان شان را در لیست دوستان خود اضافه کنند تا بتوانند ارتباطات و فعالیت های آنها را در فیس بوک پیگیری کنند.

به صورت دوره ای گزارش چت، ایمیل ها، فایل ها و محتوای صفحات، دوستان و عکس های نوجوان تان در اکانت فیس بوک اش را کنترل کنید. شفاف و روراست باشید، بگذارید که کودک تان بداند شما چنین کنترلی را انجام می دهید.

بیش از آن که پلیس فرزندان تان باشید، سعی کنید همراه و یارشان باشید. این کار آنها را به صورت یک شهروند آنلاین مسئولیت پذیر در زندگی، خانه و دانشگاه بار می آورد.

آنچه والدین باید درباره اینترنت بدانند

به فرزندان خود بیاموزید که:

•قبل از کلیک کردن به این فکر کنند که: با چه کسی در حال گفت‌وگو (chat) یا نامه‌نگاری هستند، در حال گفتن چه مطلبی هستند و از چه لحن و شیوه‌ای برا گفتن آن استفاده می‌کنند؟ آیا شخصی که در سمت دیگر این گفتگو قرار دارد متوجه شوخیهای آنها می‌شود؟

•قبل از واکنش نشان دادن به موضوع آنلاینی که موجب ناراحتی آنان شده است، میز کامپیوتر را ترک کرده و چند نفس عمیق بکشند.

•از شایعه پراکنی، همکاری در اذیت و آزار دیگران و دادن اطلاعات خصوصی و گفت‌وگوهای خودمانی در اینترنت خودداری کنند.

•قانون طلایی فضای مجازی را رعایت کنید: هرگز کاری را که در زندگی واقعی انجام نمی‌دهید، در اینترنت هم انجام ندهید.

خودتان هم موارد ایمنی را رعایت کنید:

•نرم‌افزار ضد spyware و adware را بر روی کامپیوتر خود نصب کنید.

•از سلامت و به روز بودن firewall خود اطمینان حاصل کنید.

•یک نرم افزار ضدویروس بر روی رایانه نصب کرده و آنرا به طور منظم به روز نمایید.

نکات ایمنی در سنین دبستان

زیر هشت سال

•از فناوری‌های فیلترینگ یا کنترل والدین parental control استفاده کنید. به جای فیلتر کردن سایت‌های "بد" هر موردی که با آن موافق نیستید را مسدود کنید.

•درباره اینکه آیا فرزندتان واقعا به داشتن یک آدرس ای-میل یا سیستم‌های پیام رسانی نیاز دارد، فکر کنید. اگر پاسخ مثبت است، تمام ارتباطات به غیر از فهرست گیرندگان و فرستندگان مورد تایید خود را فیلتر کنید و مراقب باشید که فهرست دوستانش، طولانیتر از رقم سنش نباشد و شما همه آنها را در زندگی واقعی، بشناسید.

•وب سایت‌های مورد علاقه آنها را در بخش نشانک یا Bookmark قرار دهید تا برای پیدا کردن آنها نام سایت را اشتباه تایپ نکرده و از سایت "بد" سر در نیاورد.

•از موتورهای جست‌وجوی کودکان مانند Yahooligans و Ask Jeeves استفاده کنید.

•زمان حضورشان در اینترنت را به نیم ساعت در روز محدود کنید، مگر اینکه در حال انجام دادن یک برنامه خاص درسی باشند.

•فعلا اجازه اسفاده از بازی‌های اینتراکتیو (interactive) مانند X-Box Live یا شبکه آنلاین (Playstation) را به آنها ندهید. در عوض به سایت‌هایی چون Toontownبروید.

•تا جایی که می‌توانید در کنارشان بنشینید و ببینید که در اینرنت به کجا می‌روند، چه چیزی برایشان جالب است و هر سوالی که فکر می‌کنید بپرسید و به تمام سوالات او پاسخ دهید.

•به آنها بگویید که قبل از فرستادن هر مطلبی اعم از مشخصات شخصی یا مطالب دیگر از طریق ایمیل، IMیا قرار دادن آن در بلاگ و وب سایت، نظر شما را جویا شوند.

•در اوقات فراغت به دنبال سایت‌های سالمی بگردید که بتوانید به او معرفی کنید. فهرستی از این سایت‌ها در WiredKids.org موجود است.

۸ تا ۱۰ سال

•اگر فرزندتان نمی‌تواند وارد سایت‌هایی که از طرف مدرسه معرفی شده یا سایت‌های مناسب با سن خود شود، میزان فیلترینگ کامپیوتر را کاهش دهید. بعضی از وب سایت‌ها مانند MSN دارای این امکان هستند که هر صفحه برای باز شدن به اجازه والدین نیاز دارد و به این منظور ای-میلی به نشانی آنها می‌فرستد و در صورت پاسخ مثبت، صفحه را باز می‌کند.

•اگر سرویس پیام فوری یا IM را فعال کرده اید، فهرست فرستندگان پیام را به اشخاص آشنا محدود کنید.

•از یک برنامه ضد pop-up یا نوارابزاری مانند گوگل استفاده کنید.

برنامه ضد ویروس و منهدم کننده نرم افزارهای جاسوس را نصب و فعال کنید زیرا دانلودهای پر ویروس از همین سنین آغاز می‌شود.

•موتورهای جست‌وجو را تغییر نداده و همچنان از Yahooligans و Ask Jeeves استفاده کنید.

•مطمئن شوید که آنها به خوبی متوجه هستند چه اطلاعاتی قابل قراردادن در اینترنت هستند و کدام اطلاعات نباید در اختیار دیگران قرار بگیرند.

•گفت‌وگوی آنلاین را با آنها تمرین کنید تا بیاموزند با غریبه های حاضر در فضای مجازی چگونه برخورد کنند.

•درباره استفاده از نرم افزارهای نظارت فکر کنید. به این وسیله میتوانید آنچه انجام می‌دهند را بررسی کنید.

•علاوه بر تهیه Back up از فایل‌ها، برنامه ضد جاسوسی کامپیوتر را مدام چک کنید. ممکن است فرزندتان هنگام کار اشتباها آن را پاک کرده یا از کار انداخته باشد.

•گذشته از موارد درسی، زمان حضور او در اینترنت را با احتساب پیام‌ها و ایمیل‌ها به کمتر از ۱ ساعت در روز محدود کنید.

نکات امنیتی که باید والدین و فرزندان بدانند

اینترنت می تواند یک منبع فوق العاده برای کودکان باشد. ایشان می توانند از آن برای کارهای پژوهشی مربوط به مدرسه شان استفاده کنند، یا با سایر هم سن و سال ها و یا معلمان شان ارتباط برقرار نمایند، و یا بازی های آموزشی آنلاین انجام دهند. کودکانی که به اندازه کافی بزرگ شده اند تا بتوانند نامه بنویسند یا تایپ کنند، می توانند به سادگی به دنیای مجازی دسترسی پیدا کنند.

اما این دسترسی می تواند همراه با تهدیدات و خطراتی باشد. برای مثال، یک کودک ۸ساله بدنبال جستجوی آنلاین برای خرید اسباب بازی (Lego)ممکن است با یک اشتباه تایپی، Legsرا تایپ کند، با این اشتباه کوچک ممکن است موتور جستجو او را به سایت هایی که روی کلمه مذکور تمرکز دارند، رهنمون سازند که ممکن است این سایت ها شامل موارد پزشکی و سایر مسائل باشد.

نکته اساسی در این مبحث اینست که باید از اینکه فرزند ما در اینترنت چه می بیند یا می شنود، با چه کسانی آشنا می شود، و چرا آنها باهم ارتباط برقرار کرده اند، آگاهی داشته باشیم.

همانند هر مساله ی امنیتی دیگر، کاملا عاقلانه است که با فرزندانمان صحبت کنیم. دلیل نگرانی های خود را بیان نماییم، مزایای حفاظت از منابع اینترنتی را برایشان آشکار کنیم و با چشمانی باز فعالیت هایشان را زیر نظر بگیریم.

همواره پیشگیری بهتر از درمان است، پس کاملا منطقی است برای حراست از فرزندانمان در مقابل کلاهبرداران و سوء استفاده گنندگان در فضای اینترنت راه حلی داشته باشیم.ما این موارد را به شما پیشنهاد می کنیم :

- کامپیوتر بلد باشید و بیاموزید چگونه برخی کاربردها را مسدود کنید.
- کامپیوتر را در فضای تردد افراد قرار دهید نه در اتاق شخصی، تا بتوانید زمان استفاده فرزندتان مانیتور را مشاهده کنید.
- با فرزندتان یک ایمیل را مشترکا استفاده کنید تا بتوانید پیام هایش را مشاهده کنید
- سایتهای مورد علاقه فرزندتان را نشانه گذاری (Book Mark)کنید تا دسترسی به آنها برایش ساده باشد.
- زمانی را صرف آموزش رفتار صحیح در فضای مجازی برای فرزندانتان کنید.
- فرزندانتان را از رفتن به اتاق های گفتگو خصوصی منع کنید، از نرم افزارهای فیلترینگ یا تنظیمات امنیتی مرورگر یا سرویس دهنده اینترنت خود برای مسدود کردن مورد فوق استفاده کنید.بدانید که ارسال پیام در یک اتاق گفتگو آدرس الکترونیکی شما را به سایرین نمایش می دهد.

- کارت های اعتباری خود را برای جلوگیری از هرگونه پرداخت های ناشناس چک کنید .
- تصور کنید چه اتفاقی می افتد، اگر بعد از مدرسه، خانه ی همکلاسی اش، یا هر مکان دیگری که فرزندان بتوانند در آنجا بدون نظارت شما به کامپیوتر دسترسی داشته باشند.
- ناراحتی فرزندتان را جدی بگیرید خصوصا اگر ناراحتی اش بابت تبادلات آنلاین است.
- کپی از پیام های تهدید آمیز یا غیراخلاقی را که فرزندتان دریافت کرده است را برای سرویس دهنده اینترنت خود ارسال کنید.
- اگر با اینگونه پیام ها یا هرگونه پیام هایی حاوی مطالب خارج از عرف مواجه شدید با وب سایت پلیس فتا به نشانی www.cyberpolice.ir مکاتبه نمایید.

در ادامه پلیس فتا توصیه های پیشگیرانه دیگری به نوجوانان عزیز پیشنهاد می کند:

- در رابطه با گفتگوها و ارتباطاتی که بابت آن نگران هستید همواره والدین خود را در جریان بگذارید.
- هرگز به پیام ها یا پستهای الکترونیکی تهدید آمیز پاسخ ندهید.
- هرگز اطلاعات شخصی خود از جمله، آدرس، شماره تلفن، نام مدرسه یا محل آن را فاش نکنید.
- از نام مستعار استفاده کنید و نیز هرگز با کسی که در اتاق گفتگو آشنا شده اید ملاقات نکنید .

نکات مهم در استفاده فرزندان از اینترنت

این دنیای آنلاین، بستری منحصر بفرد است که در آن مردم در تمام سنین می توانند در کنار هم دانش خود را افزایش دهند.

درباره اینترنت صحبت کنید و به آنها فرصت دهید که در کنار شما شبکه را کشف کند. از فرزند خود بخواهید که به شما نشان دهد چقدر به آنلاین بودن علاقه دارد و اگر تمایلات فرزندتان با شما یکی نبود سعی کنید شوکه نشوید.

خلاقیت کودک خود را تحریک کنید و فرزند خود را به سمت بهترین محتوای آنلاین هدایت کنید تا بتواند خلاقیت خود را توسعه دهد. کودک شما می تواند یاد بگیرد و سایتهای جدید را کشف کند، بازی کند، وبلاگ بنویسد، وب سایت بسازد و ... به این ترتیب می توانید تصور ذهنی فرزندتان را توسعه دهید.

در کنار هم و با یکدیگر قوانین و موانعی را بسازید و تعیین کنید که چه وقت/ کجا/ چرا و به چه مدتی فرزند شما می تواند از تلفن همراه یا رایانه استفاده کند. شما باید یاد بگیرید که به حرفهای فرزندتان گوش دهید و قوانین عادلانه ای را تدوین کنید.

اطلاعات شخصی را حفظ کرده و به فرزند خود کمک کنید بفهمد که اطلاعات و عکسهایی که در شبکه می گذارد می توانند برای همیشه و برای همه قابل رویت باشند. به کودک کمک کنید که از بالاترین سطوح حریم شخصی در شبکه های اجتماعی استفاده کند.

به استفاده از ابزارهای کنترل شخصی فکر کنید که می توانند به طور خودکار بعضی موضوعات خاص (موضوعات غیراخلاقی، خشونت و ...) را فیلتر کنند و زمان وبگردی کودک خود را محدود کنید.

از گذاشتن رایانه شخصی در اتاق کودک خود اجتناب کنید و در عوض، رایانه را در اتاق نشیمن قرار دهید. با این کار می توانید از سلایق فرزند خود در زمان

وبگردی آگاه شوید.

نرم افزار فیلترینگ خانگی برای خانواده های ایرانی

در اکثر کشورها این نرم افزار بر روی رایانه خانگی افراد نصب می شود و در کشور ما نیز فیلترینگ خانگی براساس ارزش های فرهنگی، اخلاقی و بومی کشور توسط متخصصان داخلی بخش خصوصی تهیه شده است. تشخیص خودکار و هوشمند نسبت به تصاویر از جمله ویژگی های بارز این نرم افزار است که مقطع سنی خاصی را شامل نمی شود.

همچنین اجزای این برنامه از دید والدین، تعریف فرزندان، امکان انتخاب محدوده سنی برای فرزندان، کنترل تصاویر با استفاده از روش‌های مبتنی بر هوش مصنوعی، امکان تعیین زمان استفاده، امکان تغییر پیام‌ها توسط والدین، ارائه گزارشات، امکان اعمال تنظیمات دلخواه و تغییر رمز عبور اصلی است.

نسخه جدید نرم‌افزار فیلترینگ خانگی نیز با نام "نظارت والدین بر مصرف اینترنت" با اعمال برخی تغییرات در نصب و اجرا برای دانلود رایگان در وبگاه دبیرخانه شورای عالی اطلاع رسانی ارائه شده است.

واسط کاربری کامل نرم‌افزار و نصب آن بدون نیاز به اعمال تغییرات در سیستم‌عامل نرم‌افزار انجام می‌شود، همچنین در نسخه جدید نرم‌افزار سازگاری بیشتری با ویروس‌یاب‌ها پیدا کرده است. از دیگر تغییرات اعمال شده نیز می‌توان به محافظت از غیرفعال کردن، از نصب درآوردن و تغییر تنظیمات نرم‌افزار به صورت غیرمجاز توسط کودکان اشاره کرد.

اینترنت و نقش تربیتی والدین

نوجوانی و جوانی یکی از بحرانی ترین دوران زندگی است ورود به این دوره فرد را با مشکلات فراوانی مواجه این مرحله نه تنها دوران دشواری برای نوجوانان است بلکه والدین آنها نیز در این دوران دچار فشار مالی روانی اضطراب و سایر دگرگونیها میشوند بنابراین ضروری است که والدین شیوه های ارتباطی ، انضباطی و کنترل جدیدی برای ارتباط و برخورد موثر با نوجوانان استفاده کنند. اکثر والدین می خواهند روابطشان را با فرزندشان بهبود بخشند اما بسیاری از آنها راه اینکار را نمی دانند. نه بی خیال شدن و نه سخت گیری و کنترل شدید به روابط میان فرزندان و والدینشان منتهی نمیشود. لذا هیچ یک از این دو روش ، مؤثر واقع نمی شود.

خانواده در رویارویی با اینترنت

ما در ایران با دو نوع خانواده رو به رو هستیم: خانواده مولکولی- که در آنها هیجان احساس و عواطف فرزندان بسیار مهم است.

خانواده اتمی- که در آنها ارتباطات عاطفی ، هیجانی به حد صفر رسیده در این خانواده کامپیوتر بعنوان عضوی از اعضای خانواده ، به همان دلیلی که فضای مجازی را ایجاد می کنند جوان را از بستر خانواده اش دور می کند و در واقع جوان را تخلیه روانی می کند.

در واقع این رایانه ها هستند که با ایجاد فضای مجازی رخنه را در دل خانواده ها پدید می آورند جوان امروزی بیشتر دوست دارد که چت کند و آن را یک فضای مجازی می داند والدینی که موافق با این تکنولوژی هستند ابراز می کنند که آموزش تنها انگیزه مشترک استفاده فرزندانشان از اینترنت در خانه است.

شیوه برخورد با تخلفات تربیتی

گاه با وجود تشویق و ترغیب کودک والدین به دلایلی دچار خطا و اشتباه میشوند و رفتار های ناهنجاری را در استفاده از دنیای وی از خود بروز می دهد چت ورود به سایتهای غیرمجاز ارتباط با افراد غریبه ، مشکوک و ... در این موقعیتهای نابهنجار برخی از والدین بلافاصله اقدام به مجازات و ملامت فرزند خود می نمایند از نظر مربیان مسلمان رویه ای قابل قبول نیست و چه بسا که این نوع رفتارها کودک را نسبت به رفتارهای خود جری می کند.

حمایت از کودکان در مواجهه با آسیبهای اینترنت پیشرفت در فناوری اطلاعات و ارتباطات و گسترش آن در تمام شئون زندگی انسان روند زندگی فردی و اجتماعی را دگرگون ساخته است ، اینترنت با ارایه فضایی آزاد و بی در و پیکر به افراد آزادی می دهد کودکان بعنوان بخشی از کاربران اینترنت از آسیبهای احتمالی آن در امان نیستند. آسیبهای اینترنتی را از نظر فرهنگی و اجتماعی ؛فرهنگی ؛

ترویج فساد اخلاقی و بی بندوباری با توجه به وجود سایتهای مبتذل و مستهجن ، ایجاد رخنه در مبانی و اصول ادیان الهی ، دین مبین اسلام و بعضا بی احترامی به مقدسات . اجتماعی - اشغال اوقات فراغت و فرصتهای جوانان و هدررفتن سرمایه های مالی.

-تغییر تدریجی بنیانهای خانواده با ترویج بی بند و باری

والدین باید توجه داشته باشند که در خصوص مواجهه با آسیبها میبایست سطح درک دانش خود را نسبت به اطلاعات وسیعی که در اینترنت وجود دارد را بالا برده تا بعنوان یک رهنمای خوب آداب و اخلاق اسلامی و انسانی و مسئولیت پذیری کودکان خود را به سمت و سوی درست و روحانی هدایت نمایند. راه هایی برای حفظ کودکان - بالا بردن و ارتقاء فرهنگ استفاده از اینترنت - استفاده از فلیترهای مناسب در جهت سالم سازی فضای مجازی - مشخص نمودن ساعت استفاده از اینترنت در محیط خانواده

-اطلاع رسانی سایتهای مفید و سودمند

- سهیم شدن کودکان با والدین در فعالیتهای اینترنتی و آگاهی از روشها و رفتارهای کودکان توسط والدین

-به فرزندانمان بیاموزیم که اگر در مورد موضوعی از موضوعات اینترنتی احساس ناخوشایندی دارند حتما با والدین در میان بگذارند

- به فرزندانمان آموزش دهیم که هر اطلاعاتی را از طریق اینترنت ارسال ننمایند

- به کودکان یا آور شویم که تفاوت بین درست و غلط در اینترنت همانی است که در دنیای واقعی وجود دارد

- به کودکان مان خاطر نشان کنیم که هر آنچه را در اینترنت می بینند و یا می خوانند صحیح نیست و مطالب را با شما در میان بگذارند

- به فرزندانمان یاد دهیم که به حقوق سایر کاربران در اینترنت احترام بگذارند

- والدین به فرزاندان خود بیاموزند که از بازکردن ایمیل های افرادناشناخته خودداری کنند تا معضلات اینترنتی برای فرزندان فراهم نشود.

- اگر کودکان ساعات بیشتری را از آنچه که والدین تمایل دارند صرف استفاده از اینترنت می کنند جهت دهی و مدیریت شود.

باید و نبایدهای استفاده فرزندان از اینترنت

نمی توان از کودکان خواست وارد اینترنت نشوند؛ نوجوانان از جمله کاربران اصلی اینترنت هستند و علاقه زیادی دارند از طریق (چت روم) در اینترنت با دیگران گفتگو کنند اما آنچه اهمیت دارد استفاده صحیح آنان از این وسیله ارتباطی است.
به گزارش خبرگزاری آریا ، پلیس فتا توصیه هایی درباره چگونگی استفاده صحیح فرزندانمان از اینترنت ارائه نمود:

۱- با فرزندان خود درباره آنچه در اینترنت انجام می دهند صحبت کنید و آنها را تشویق کنید به هنگام گشت و گذار در اینترنت ، پدر و مادر، آموزگار یا سرپرست خود را در جریان بگذارند .

۲- متخصصین و کارشناسان توصیه می کنند رایانه ای که کودک از آن استفاده می کند باید در نشیمن گاه خانه، جایی که والدین و سرپرستان بر آن نظارت دارند قرار داده شود . این اقدام کودکان را تشویق می کند وقتی به مساله نگران کننده ای برخورد کردند بزرگتر ها را در جریان بگذارند.

۳- بکارگیری نرم افزارهایی که به والدین امکان دهد محتویات اینترنت را کنترل کنند می تواند مفید باشد، برخی فیلترگذاری ها پیش پا افتاده است و سایت های مفید را نیز مسدود می کند.

۴- بسیاری از والدین بیش از پیش نگران پیام های نامناسبی هستند که به صندوق ایمیل کودکان ارسال می شود . این پدیده ناشی از این واقعیت است که محصولات پورنوگرافی از جمله شایع ترین انواع ایمیل های تبلیغاتی است .

۵- یکی از راه های پرهیز از این دردسر ایجاد دو آدرس ایمیل برای کودکان است. یکی از این آدرس ها، ایمیل خصوصی است که برای ارسال پیام با آشنایان و دوستان کودک مورد استفاده قرار می گیرد و دیگری یک آدرس عمومی است برای گشت و گذار در اینترنت و ثبت در وب سایت های مختلف ؛ به این ترتیب ایمیل های ناخواسته، وارد صندوق عمومی خواهد شد و والدین می توانند آن را کنترل کنند .

۶- کودک باید احتیاط زیادی به خرج دهد و هر بار پیش از ورود به چت روم های محلی از والدین خود اجازه بگیرد ، حتی اگر یک چت روم مختص ورود کودکان باشد. در حال حاضر هیچ راهی برای جلوگیری از ورود بزرگسالان به آن وجود ندارد . ممکن است کسی برای اغفال کودکان به آن وارد شود .

۷- کودکان هرگز نباید آدرس منزل ، شماره تلفن یا نام مدرسه محل تحصیل خود را در اختیار کسانی بگذارند که در اینترنت ملاقات می کنند مگر آن که به طور مشخص از پدر و مادر یا آموزگار اجازه داشته باشد .

۸- نباید بدون اجازه پدر و مادر یا سرپرست خود ، مشخصات کارت اعتباری یا اطلاعات بانکی خود را برای کسی ارسال کنند . همچنین کودکان باید کلمات گذر (password) را کاملا مخفی نگاه دارند و حتی در اختیار نزدیک ترین دوست خود قرار ندهند .

۹- کودکان نباید از نام خانوادگی به عنوان کلمه گذر استفاده کنند چون حدس زدن آنها آسان است . در عوض توصیه می شود از حروف و ارقام به صورت ترکیبی استفاده شود .

۱۰- هرگز به کودکان اجازه ندهید بدون اجازه شما شخصا با کسی که در اینترنت با او آشنا شده است ملاقات کند؛ در صورت ضروری بودن ، باید با یکی از بزرگسالان خود و در اماکن عمومی این ملاقات صورت پذیرد .

۱۱- کسانی که در اینترنت با کودکان تماس می گیرند همیشه افرادی نیستند که ادعا می کنند .

چگونه با استفاده نادرست فرزند خود از اینترنت برخورد کنیم؟

برخی از والدین از این که فرزندشان از کامپیوتر و اینترنت به هر میزان و بدون محدودیت استفاده می کند حتی احساس غرور و مباهات می کنند و اجازه می دهند که رفتار تا جایی پیش برود که صدمات جبران نشدنی به روابط، درس و روحیه اش بزند و به علاوه رفتارش هم به قدری تثبیت شود که تغییر آن دشوار باشد.

در سوی دیگر این تایید کامل و سهل انگاری، برخوردهای شدید و قهرآمیز و از جمله کشیدن دو شاخه کامپیوتر از برق، دعوا با فرزند و کنترل شدید او است. این روش هم معمولا دوامی ندارد و به علاوه عوارض فراوانی دارد که مهمترین آن ها، تخریب ارتباط والدین و فرزندان است.

قبل از رو به رو شدن با فرزندی که استفاده افراطی از کامپیوتر و اینترنت می کند اول باید خود والدین تکلیفشان را انجام دهند، زمانی که واقعا فرزندان صرف کامپیوتر و اینترنت می کنند، تا حد امکان دقیق و محاسبه کنند، چه موقعی والدین در منزل هستند و چه زمانی نیستند و فرزند پای کامپیوتر است.

به دور از اغراق و مبالغه و کلی گویی که متاسفانه ما ایرانی ها چنین عادتی را زیاد داریم و بهتر است به ارقام و اعداد بیشتر توجه شود. مثلا به فرزندمان می گوییم که از صح تا شب توی اینترنتی که به واقع چنین نیست. با محاسبه و برآورد دقیق هم خودمان به یک آگاهی درست و شاید آرام بخش می رسیم و هم به فرزندمان نشان می دهیم که قصد اتهام زدن و سرزنش نداریم. به مشکل توجه دقیق و کافی داریم و او هم دیگر ما را متهم نمی کند که از میزان استفاده او بی اطلاع هستیم.

جلوگیری از جنگ و جدال دائمی برسر مشکل، در نهایت باید به اصول و قوانینی عملی و قابل اجرا برسیم. طبعا هر چه سن فرزند ما بالاتر می رود این اصول باید دو طرفه و توافقی تر باشد. شرکت فرزند در وضع این اصول و قوانین یک طرفه و تحصیلی بودن آنها را کم تر و اجرای آنها را آسان تر می کند.

این اصول می توانند در قالب قوانین و جدول استفاده از اینترنت مطرح شود. برنامه و جدولی که دقیقا معلوم می کند در ساعت فلان در فلان روزهای هفته و با رعایت این اصول و قوانین، کامپیوتر، گیم یا اینترنت برای فرزند قابل استفاده است و مثلا در صورت تخطی، او از استفاده از آن یا از فعالیت مورد علاقه دیگر محروم خواهد شد. بعد از طراحی جدول و قوانین و توافق هر دو طرف، آن ها را سرسختانه و بدون مسامحه و کوتاهی اجرا کنیم.

آسیب هایی که فرزندان را تهدید می‌کند

نوجوانان و جوانان گمشده‌ها و کمبودهای عاطفی خود را در بازی‌های پرهیجان و بی محتوای رایانه ای، موسیقی های مبتذل غربی و فضای پرخطر و مجازی اینترنت جست و جو می کنند؛ آنها در یک گمان واهی بر این باوراند که کامپیوتر و اینترنت دروازه ورودشان به دنیای اطراف است.

دغدغه هر پدر و مادری داشتن فرزند یا فرزندانی سالم و تندرست است. والدین بیش از هر چیز نگران خورد و خوراک، پوشاک، درس و مشق بچه‌ها هستند و برای برآورده کردن این نیازها است که شب و روز تلاش می کنند و لحظه‌ای آرام و قرار ندارند، اما آیا هیچ با خود اندیشیده‌اید که دلبندان‌مان علاوه بر غذای جسم به غذای روح و روان هم احتیاج دارند که اگر چنانچه این غذا در فضای گرم و صمیمی و در محیط خانواده برایشان فراهم نشود خود را برای تهیه این غذاها به هر در و دیواری می‌زنند یا با هر طناب پوسیده‌ای به قعر چاه می‌روند و آینده خود را تباه می‌سازند.

امروزه با گسترش وسائل ارتباط جمعی متأسفانه نوجوانان و جوانان گمشده‌ها و کمبودهای عاطفی خود را در بازی‌های پرهیجان و بی محتوای رایانه ای، موسیقی های مبتذل غربی و فضای پرخطر و مجازی اینترنت جست و جو می کنند. آنها در یک گمان واهی بر این باوراند که کامپیوتر و اینترنت دروازه ورودشان به دنیای اطراف است و ما به عنوان والدین اگر لحظه ای، فقط لحظه ای غفلت کنیم فرزندان خود را غرق در خطر می بینیم و اگر مدیریتی صحیح و نظارتی دقیق بر کارها و رفتار آنها نداشته باشیم نوجوانان مان همچون ماهی از دست مان سر می خورند و در دریای پرتلاطم امواج ماهواره و اینترنت غرق می شوند. آن موقع است که رهایی آنها از این دام ها کاری بس دشوار خواهد بود.

رایانه، اعتیاد جدید قرن

امروزه دنیای رایانه هویت یابی و هویت جویی نسل جوان را تا جایی در ابعاد فکری و اخلاقی تحت تأثیر قرار داده که آسیب های اجتماعی رابطه تنگاتنگ با مقوله فناوری اطلاعات، انفجار اطلاعات و جهانی شدن پیدا کرده است.

"رضا نباتی"، کارشناس فرهنگی در گفت وگویی با بیان این موضوع که رایانه موجب بروز پدیده جدید "اعتیاد نو و مدرن" و افزایش آسیب‌های اجتماعی شده است، خاطرنشان می کند: «استفاده خارج از حد متعارف از اینترنت باعث وابستگی شدید روانی و فکری کاربر می شود. به طوری که بعضی از کاربران به یک فضای غیرواقعی پناه برده و در آن زندگی می کنند. در این میان سودجویان نیز از طریق اینترنت به راحتی کالاهایشان را تبلیغ می کنند، خبرهای دروغین و پیام های مورد نظرشان را برای جوامع می‌فرستند، ابهت فرهنگی و دینی خانواده‌ها را می‌شکنند و زمینه‌های آشفتگی هویت را برای نوجوانان فراهم می‌کنند».

این کارشناس تأکید می‌کند: «آنان در این بین با کوچک‌ترین غفلت و ناآگاهی والدین، راه را برای انواع انحرافات و آسیب های اخلاقی، فرهنگی فرزندان جامعه باز کرده و موجب سقوط آنان از درجات بلند معنویت خواهند شد .

وی در خصوص راهکارهای برخورد با این مشکلات و مناسب ترین برخورد والدین با نوجوانان و جوانان با شروع تعریفی از آسیب، می‌گوید: «عواملی که موجب دور شدن فعالیت‌های اجتماعی نوجوانان از مسیر تربیت و حضور در رفتارهایی که می‌تواند به او در پیدا کردن مسیری مناسب صدمه بزند، آسیب نامیده می شود. همچنین آسیب‌های نوپدید هم آسیب‌هایی هستند که از ارتباط نوجوانان با ابزار و تکنولوژی‌های جدید ممکن است برای او پیش آید و مسیر تحصیل، تربیت و آینده او را از جهت اصلی دور کند .بنابراین یکی از راه‌های پیشگیری از بروز این گونه آسیب‌ها در نوجوانان توجه ویژه به تربیت و تقویت مسائل دینی و مذهبی آنها از سوی مسئولان آموزشی و تربیتی و مخصوصاً خانواده‌ها است .ضمن این که نقش مدیریتی والدین را هم در نحوه استفاده صحیح از این ابزار نباید نادیده گرفت.

نباتی با اشاره به این که خودباوری ضعیف در نوجوانان و عدم توجه به نیازهای عاطفی و احساسی در سنین بلوغ از سوی خانواده زمینه گرایش آن‌ها را به سوی

اعتیاد فراهم می‌کند، می‌گوید: «اگر اولیا و مربیان آموزشی این اجازه را به نوجوان بدهند که هر کدام با توانمندی هایی که دارند به موقعیت‌های مناسب و صحیحی دست یابند و این احساس "من می توانم خوب باشم" را در خود ببینند، اعتماد به نفس و باور جوان و نوجوان از خودش در سطح بسیار خوبی قرار می‌گیرد و اگر نوجوانی خود را باور داشته باشد و ارزش خاصی برای خود قائل باشد کمتر تحت تأثیر دیگران، عوامل بیرونی و فضای مجازی قرار می‌گیرد».

جوانی، دنیایی سرشار از تحرک

دنیای جوانی و نوجوانی، دنیای هیجان و تحرک، شور و نشاط و شادی است. امروزه در برخی از خانواده‌ها این هیجانات و تحرکات با شنیدن موسیقی‌های غربی از طریق ماهواره و سی دی، تخلیه می‌شود. البته موسیقی به خودی خود آسیب‌زا نیست، اما وقتی موسیقی با چاشنی زیرزمینی و آهنگ‌های غربی مثل رپ، متال و... همراه شود، آن وقت است که باید گفت خطری جدی خانواده‌ها را تهدید می‌کند؛ چرا که گرایش نوجوانان به موسیقی‌های مبتذل زمینه ورود آنها را به انحرافات اجتماعی از قبیل اعتیاد و گرفتار شدن در دام‌های مصیبت بار را فراهم می‌سازد.

حال این که چگونه موسیقی به عنوان یکی از ابزارها باعث اعتیاد در نوجوانان و جوانان می‌شود، سؤالی است که حسین سیرانی، روان شناس و مدرس دوره‌های مهارت‌های زندگی به آن پاسخ می‌دهد. وی در گفت وگویی با اشاره به اینکه افراد در موقعیت‌های متفاوت واکنش‌های مختلفی از خود نشان می‌دهند، می‌گوید : »هر وقت تعادل جسمی، روانی و اجتماعی نوجوانان در برابر موقعیت‌ها به هم بریزد، آسیب شروع می‌شود .گوش انسان و حس شنوایی او یکی از حواسی است که اگر تعادل آن از بین رود، آسیبی جدی متوجه فرد می‌شود. مقدار صدایی که قرار است هر کس بشنود می‌تواند به او آرامش دهد یا این که آسیب ایجاد کند و اگر در این بین سیستم عصبی هوشمند خود را به خوبی بشناسیم و کارایی آن را بدانیم، قطعاً کمتر دچار آسیب های متعدد می شویم».

این روان شناس با بیان این که به طور متوسط میلیاردها سلول عصبی هوشمند در بدن و مغز انسان ها وجود دارند، می گوید: «این سلول‌های عصبی هوشمند وظایف متعددی را برعهده دارند که از جمله انتقال پیام‌های عصبی به سیستم عصبی خودکار یا مغز می باشد که به طور طبیعی یک سرعت زمانی خاص برای انتقال این پیام‌ها در نظر گرفته شده است، چنانچه این زمان کاهش یا افزایش یابد، سیستم عصبی دچار اختلال می‌شود و فرد برای رفع این اختلال نیاز به کمک‌های حمایتی دارد که گاهی محرک بیشتر یکی از آنها می‌باشد که این محرک می‌تواند موسیقی باشد».

سیرانی می گوید» :گوش انسان به طور طبیعی با شنیدن صدای طبیعت آرامش پیدا می‌کند، اما با شنیدن موسیقی هایی که صدای آنها از حد طبیعی خارج هستند همچون موسیقی زیرزمینی که به سبک متال، هوی و رپ تولید می‌شوند، باعث می‌شود سرعت طبیعی درک صوتی از حد طبیعی خارج شده و شدت پیدا کند بر همین اساس است وقتی فرد به موسیقی تند گوش می دهد احساس هیجان و نشاط پیدا می‌کند، این نشاط بیش از حد فقط برای مدت کوتاهی در وی هیجان دارد و بعد از تکرار سلول‌های عصبی از دریافت و انتقال این پیام‌های زیاد و سریع خسته می‌شوند و حالت عصبی و پرخاشگری را به طور ناخودآگاه در فرد ایجاد می‌کنند و به اصطلاح فرد جرقه‌ای می‌شود و از کوره درمی‌رود .در ادامه فرد جرقه‌ای شده مدام خسته‌تر می‌شود و واکنش‌های هیجانی یا خوشحالی دیگر از خود نشان نمی‌دهد و به مرور زمان برای درس خواندن و انجام کارهای روزمره نیز به مشکل برخورده و با کم حوصلگی و عدم تمرکز بر روی کارها مواجه می‌شود که شایع‌ترین آنها "پرش افکار" است.

این مدرس می‌گوید: «در این زمان است که فرد برای ادامه فعالیت‌های خود کما فی السابق به محرک دیگری روی می‌آورد تا بتواند به حالت نرمال گذشته برگردد. در این موقع است که نیاز به دوپینگ کردن پیدا می‌کند. چنانچه برای این شارژ شدن در محیطی قرار داشته باشد که این شرایط به آسانی برای او فراهم شود، به راحتی از آن استفاده خواهد کرد. در غیر این صورت با راهنمایی و کمک دوستان درصدد راه چاره‌ای برمی آید و از همین جاست که پای او به جاده خطرناک اعتیاد باز می‌شود.

این روانشناس خاطرنشان می‌کند: «یک نوجوان یا جوان با یک بار مصرف مواد مخدر معتاد نمی‌شود، بلکه در وهله اول او نشاط بیشتری نیز می یابد، در مرحله بعد جمع گراتر می‌شود و به قول معروف سرحال می‌شود، و شاید حوصله‌اش هم برای انجام کارها بیشتر شود، اما این آغاز راه اعتیاد است، چون تا زمانی که اثر

ماده در بدن فرد وجود دارد او قدرت و توانایی دارد و این روند آرام آرام کاهش می‌یابد تا جایی که او همان آدم قبلی نیازمند به محرک می‌شود«.

وی می گوید: «با توجه به این که فرد، تجربه خوشایندی را کسب کرده دوباره سراغ همان عمل می رود تا انرژی مضاعفی بگیرد و چون سرعت حرکت سلول های عصبی انتقال پیام به صورت مصنوعی افزایش یافته است، این دفعه تداوم آن شور و نشاط کم تر از دفعه قبل است و این چنین است که فرد آرام آرام برای تأمین انرژی مورد نیاز خود دز ماده را بالا برده و این چرخه آن قدر تکرار می شود تا فرد به مواد مخدر معتاد می گردد«.

سیرانی اضافه می‌کند: «موسیقی مخرب غربی به گونه‌ای فرد را به هیجان می‌رساند که درنهایت به سمت مواد مخدر سوق داده شود و افکار و عقاید مورد نیاز استعمارگران را از فرد معتاد به دست آورند.

وی با اشاره به استفاده بی رویه نوجوانان و جوانان از هندزفری برای گوش کردن آهنگ‌ها و موسیقی‌های تند به آلودگی صوتی بیش از حد آن‌ها اشاره می‌کند و می‌گوید: «ضرب آهنگ و دسیبل این موسیقی‌ها چندین برابر شدیدتر از صدای بوق ماشین، موتور و آلودگی صوتی موجود در کوچه و خیابان است که به طور غیرمستقیم به گوش می‌رسد و متأسفانه الآن گوش کردن آهنگ از طریق این گوشی‌ها بسیار رایج شده است. خانواده‌ها باید از هر حیث متوجه سلامت جسم و روان فرزندان خود باشند، تا خدای ناکرده در دام اعتیاد از طریق موسیقی‌های زیرزمینی، گرفتار نشوند؛ چرا که گسترش این فرهنگ موسیقی در جوامع جهان سوم و رو به توسعه به شدت در حال افزایش است. مخصوصا دشمنان داخلی و خارجی از طریق دشمنی خاموش به کشورهایی که از منابع ثروت زیاد ملی، معدنی و انسانی برخوردارند (مثل ایران) هجوم می‌آورند و آنها را سخت تحت تأثیر قرار می‌دهند. بنابراین مسئولان فرهنگی و مربیان تربیتی باید موسیقی های اصیل ایرانی و آهنگ های مجاز را به شکلی در اختیار نوجوانان و جوانان قرار دهند که مورد پسند آنها قرار گیرد تا راه ورود موسیقی های زیرزمینی بسته شود.

سیرانی با اشاره به این که در نوجوانان باید علامت سؤال ایجاد کرد و آزادی تصمیم گیری به آنها داد، می‌گوید: «نوجوانانی که ما فکر می کنیم از اعتقادات دینی و اصول ریشه ای خانواده دور هستند، در واقع این گونه نیستند، بلکه آن ها دنبال نگاه متفاوت اند و بهتر است این نگاه متفاوت به آن ها عرضه شود، آن موقع چیزی در جامعه و بین نسل ها اتفاق می افتد به نام "همدلی" که ما را به سمت بهداشت روانی، جسمی و اخلاقی در جامعه پیش می برد. هیچ انسانی نمی خواهد به خودش آسیب رساند، مگر این که ناآگاه باشد، بنابراین از خانواده ها و جوانان می خواهیم به سمت واژه همدلی پیش روند«.

موسیقی های کفرآمیز شیطانی

سیرانی درخصوص مضامین و متن اشعار موسیقی های زیرزمینی توضیحاتی می گوید: «متن اشعار موسیقی های زیرزمینی غربی کلماتی کاملا کفرآمیز، شیطانی و تحریک آمیز است که سلسله اعصاب و هورمون های جنسی را سخت تحت تأثیر قرار می دهد و متأسفانه به شکلی بسیار هنرمندانه طراحی شده اند که روی ناخودآگاه انسان تأثیر می گذارد و رفتار فرد را تحت اختیار خود درمی آورد.

شب نشینی های جوانان ممنوع!

یکی از آسیب هایی که جوانان و نوجوانان را تهدید می کند اعتیاد به الکل و مواد مخدر است که اکثرا در شب نشینی ها اتفاق می افتد.

دکتر حمید جمشیدیان، روان شناس با اشاره به این که اکثر آسیب ها از دوره نوجوانی و جوانی در جمع و گروه همسالان رخ می دهد، می‌گوید: «متأسفانه به دلیل این که زمینه های گرایش نوجوانان و جوانان به سمت این مواد از سوی رسانه ها، مسئولان و مربیان آموزشی به صورت مستقیم برای آن ها تفهیم و بازگو نشده است و نوجوانان در این گونه موارد با نقصان جدی روبه رو هستند، خیلی راحت در دام اعتیاد گرفتار می شوند.

دکتر جمشیدیان همچنین به نقش کم رنگ خانواده ها در جلوگیری از حضور فرزندان خود در جمع دوستان کم تجربه و کم سن و سال اشاره می کند و می گوید: «خانواده ها در جلوگیری از ورود بچه ها به وادی اعتیاد خیلی نقش دارند، اما به نظر می رسد آن ها از این خطری که جامعه و فرزندان شان را تهدید می

کند، خیلی آگاه نیستند و به واسطه مشغله زیاد کاری و نگرانی های معیشتی و شاید به دلیل عدم توانایی در برقراری ارتباط خوب با فرزندان، وظیفه اصلی خود را تا حدودی فراموش کرده اند و نمی توانند به خوبی ایفای نقش تربیتی کنند.

این روان شناس به نقش فراموش شده و کم رنگ مسئولان آموزشی هم اشاره می کند و می گوید» :بچه ها از ۲۰ درصد هوش منطقی (آی کیو) و ۸۰ درصد هوش عاطفی (ای کیو) برخوردار هستند و متأسفانه اکثر مسئولان و مربیان مدارس به هوش منطقی دانش آموزان توجه دارند و از اعتماد به نفس دادن به بچه ها و ترسیم چشم انداز آینده آنها غفلت می ورزند .اگر خانواده ها و مربیان مدارس به هوش عاطفی نوجوانان و جوانان توجه ویژه ای داشته باشند و تمام هم و غم خود را صرف آموزش دروس نکنند و آنها را از نظر عاطفی غنی سازند فرزندان را به طور طبیعی به سوی یادگیری سوق می دهند«.

دکتر جمشیدیان می گوید: «اولویت های آموزشی باید تغییر کند و خلأهای احساسی و عاطفی بین نوجوان و خانواده و مدرسه پر گردد، چنانچه به نیازهای عاطفی یک دانش آموز توجه شود، به اعتماد نفس دادن به او کمک می شود و نوجوانی که از یک اعتماد به نفس و شناخت واقعی نسبت به محیط پیرامون خود برخوردار باشد، به هیجانات و لذت های زودگذر دل خوش نمی کند و حتی درصدد یک بار امتحان کردن هم برنمی آید .چون می داند هیجان و تجربه اول بسیار خطرناک است.

راهنمای والدین با توجه به رده سنی فرزندان

آیا کودکانتان در آغاز اتصال به اینترنت قرار دارند یا تجربه کار با وب را دارند؟ در هر صورت شما می توانید آنها را در استفاده از اینترنت، همچنان که رشد می کنند و در گروه های سنی متفاوتی قرار می گیرند، راهنمایی کنید.

این مقاله به شما کمک می کند که بفهمید کودکان در سنین مختلف از اینترنت چه استفاده هایی می کنند. بنابراین شما می توانید درباره آنچه که به بهبود امنیت کودکانتان در استفاده از اینترنت کمک می کند، بیشتر بیاموزید.

سنین ۲ تا ۴ سالگی:

در طی این دوره، استفاده از اینترنت مستلزم حضور والدین است. والدین می توانند کودکانشان را روی پای خود بنشانند و به عکس های خانوادگی نگاه کنند، از یک دوربین وب برای ارتباط با خویشاوندان استفاده کنند و یا به سایت هایی که مخصوص کودکان طراحی شده، سر بزنند.

سنین ۵ تا ۶ سالگی:

زمانی که کودکان به ۵ سالگی می رسند، احتمالاً خودشان می خواهند به مکاشفه در اینترنت بپردازند. مهم است که والدین کودکانشان را برای حرکت در اینترنت به صورت امن تر در هنگامی که کودکان استفاده از اینترنت را به تنهایی آغاز می کنند، راهنمایی کنند. بعضی از سایت ها نیز برای این گروه سنی کودکان یعنی زیر ۸ سال طراحی شده اند و ابزار مناسبی برای جستجو در اختیار کودکان قرار می دهند.

سنین ۷ تا ۸ سالگی:

بخشی از رفتار طبیعی کودکان در این گروه سنی این است که کمی شیطنت کنند. مثلاً در هنگام اتصال به اینترنت این رفتار ممکن است شامل رفتن به سایت ها یا اتاق های گفتگویی شود که والدینشان اجازه نداده اند. گزارش های فعالیت های آنلاین می تواند بخصوص در طول این سنین، مفید باشد. کودکان احساس نخواهند کرد که والدینشان آنها را تحت نظر دارند، اما گزارش نشان می دهد که آنها به کجا سر زده اند. این گروه از کودکان همچنان از استفاده از سایت های مخصوص خودشان احساس خوشایندی دارند.

سنین ۹ تا ۱۲ سالگی:

در دوران قبل از نوجوانی، کودکان می خواهند از هرچیزی سر دربیاورند . آنها در مورد آنچه که در اینترنت موجود است، شنیده اند. طبیعی است که سعی کنند آنچه را که وجود دارد، ببینند. والدین می توانند با استفاده از ابزارهای کنترلی جهت کنترل دسترسی و یا مسدود سازی بعضی سایتها و موضوعات استفاده کنند. این گروه هنوز می توانند از سایت های مخصوص کودکان ۸ تا ۱۳ سال استفاده کنند.

سنین ۱۳ تا ۱۷ سالگی

کمک به نوجوانان برای امنیت در مقابل اینترنت، احتیاج به مهارت خاصی دارد، زیرا آنها اغلب در زمینه نرم افزارهای اینترنتی بیشتر از والدین خود می دانند. والدین باید نقش فعال تری در هدایت کودکان بزرگتر برای استفاده از اینترنت برعهده گیرند. رعایت جدی قوانینی که بر سر آنها بین کودکان و والدین موافقت صورت گرفته و مرور مرتب گزارش های فعالیت های آنلاین فرزندان بسیار مهم است. والدین باید بخاطر داشته باشند که باید کلمات عبور خود را محافظت کنند، تا نوجوانان نتوانند بعنوان والدین در جایی وارد شوند.

الفبای امنیت آنلاین برای تازه‌کاران در هر سنّ و سال

همکار شما، شریک شما، خانواده‌ی شما، بستگان سببی شما یا پدربزرگ‌ها و مادربزرگ‌های شما ممکن است به تازگی کار با رایانه و اینترنت را آغاز کرده باشند. ممکن است آن‌ها به اندازه‌ای که شما فکر می‌کنید زرنگ نباشند و ممکن است قربانی کلاهبرداری‌های آنلاین و حملات سایبری قرار بگیرند. به هر حال، به یک راهنمایی مختصر از شما نیاز دارند. گفتگوی شما درباره‌ی امنیت وب بایستی شامل موارد ذیل باشد:

الف) ویروس‌ها، جاسوس‌افزارها و هکرها

اگر شما می‌خواهید تعریف این عبارات را پیدا کنید می‌توانید آن‌ها را به راحتی از طریق جستجوهای آنلاین در واژه‌نامه‌های تخصّصی در موتورهای جستجو بیابید.

ب) خطرات سرقت هویّت و فیشینگ

فیشینگ: جعل مجرمانه وب‌سایت یا ایمیل یک شخص یا شرکت و یا سازمان قانونی برای سرقت رمز عبور و شماره کارت‌های بانکی است. ایده‌ی خوبی است که شما از خدمات آنلاین استفاده کنید، امّا باید مطمئن باشید که مدام وضعیت کارت بانکی و صورت حساب‌هایی که از سوی بانک صادر می‌شود را چک می‌کنید.

ج) اهمیّت محتاط بودن در زمان دانلود آیتم‌های رایگان

به کسانی که دوست‌شان دارید یادآوری کنید که طبق ضرب‌المثل قدیمی هرچیزی قیمتی دارد، حتّی اگر رایگان باشد! (هیچ ارزانی‌ای بی‌دلیل نیست!) بنابر این به آن‌ها هشدار دهید که اگر این نرم‌افزارها را دانلود کنند، ممکن است با تبلیغ‌افزارها و جاسوس‌افزارها در آن برنامه مواجه شوند.

الفبای امنیت آنلاین برای خردسالان ۳ تا ۷ ساله

الف) با خردسالان صحبت کنید

وقتی که با خردسالان درباره امنیت اینترنت صحبت می‌کنید، این کار را در حالی انجام دهید که رایانه را خاموش کرده‌اید که تمام حواس او را به خود معطوف کنید. صحبت خود را با بیان این مطلب آغاز کنید که رایانه یک ابزار است و اینترنت نیز شبیه یک کتابخانه‌ی الکترونیکی فوق‌العاده بزرگ و سرشار از اطّلاعات است.

تشریح کنید که چرا امن بودن در فضای آنلاین اهمیّت دارد. به آن‌ها بگویید که رایانه می‌تواند به مثابه‌ی یک در گشوده در برابر اطّلاعات مهم شخصی شما باشد. به آن‌ها بگویید که چطور آدم‌بدها می‌توانند کنترل رایانه‌ی شما را در دست بگیرند و آن را نابود کنند تا جایی که شما مجبور می‌شوید یک رایانه‌ی تازه بخرید.

برای آن‌ها بیان کنید که چرا اهمیت دارد که اطّلاعات شخصی خود را با افراد آنلاین به اشتراک نگذارند. به آن‌ها بگویید که از اسامی واقعی‌شان استفاده نکنند و درباره‌ی جایی که در آن زندگی می‌کنند یا مدرسه‌ای که می‌روند، صحبت نکنند.

ب) یک لیست ویژه از قوانین کاربری رایانه برای خردسالان درست کنید

این لیست باید شامل این موارد باشد:

-موزیک یا برنامه‌ای را بدون اجازه‌ی والدین از سایت‌های اینترنتی دانلود نکنید.

-تنها از اطاق‌های گفتگوی نظارت شده مثل اطاق‌های مجازی دیزنی استفاده کنید که یک بزرگ‌سال فضای چت را کنترل می‌کند.

-هرگز عکسی از خود را بدون این که قبلاً آن را با والدین در میان بگذارید، ارسال نکنید.

-از کلمات و الفاظ بد و رکیک استفاده نکنید.

-سایت‌های مخصوص بزرگ‌سالان را مشاهده نکنید.

-اطّلاعات خود را تنها با کسانی به اشتراک بگذارید که آن‌ها را در دنیای واقعی می‌شناسید. مثل هم‌کلاسی‌ها، دوستان و اعضای خانواده.

-هرگز به فرم‌ها و پرسش‌نامه‌های آنلاین بدون کمک والدین پاسخ ندهید.

-تنها از موتورهای جستجوی ویژه کودکان مثل موتور جستجوی ASK برای کودکان و «یاهو! بچّه‌ها» استفاده کنید.

ج) از مرورگرها و موتورهای جستجویی که اختصاصاً برای کودکان طرّاحی شده‌اند استفاده کنید.

مطمئن شوید که فرزندان شما از مرورگرهایی استفاده می‌کنند که کلمات و تصاویر نامناسب را نمایش نمی‌دهند. کنترل کنید که این مرورگرها تنظیمات مرتبط با مشاهده‌ی وب‌سایت‌های ایمن و مطمئن و فیلتر کلمات نامناسب را دارا باشند. تمام آن‌چه که نیاز دارید آن است که این نرم‌افزارها را بررسی کرده و تنظیمات وب‌سایت‌های پیش‌گزیده و کلمات را تایید کنید.

الفبای امنیت آنلاین برای نونهالان ۸ تا ۱۲ ساله

الف) با نونهالان خود صحبت کنید

کودکانی که در سنین هشت تا دوازده سال قرار می‌گیرند به مراتب پیچیده‌تر از زمان کودکی خود هستند. واژه‌ی کودک به دقّت منعکس‌کننده جمعیتی از بچّه‌هاست که هنوز نمی‌توان واژه‌ی نوجوان را به آنان اطلاق کرد. بدانید که کودکان در استفاده از رایانه، چه در مدرسه و چه در خانه به مراتب راحت‌تر هستند. پیش از این که شما با کودکان صحبت کنید، نیازمند این هستید که تصمیماتی را راجع به ایجاد مرزهای استفاده از اینترنت اتّخاذ کنید. برای این‌که این قوانین را وضع کنید، لازم است که آن‌ها را ابتدا تعریف کنید. برای کمک به ایمن نگه‌داشتن کودکانتان، شما بایستی به سؤال‌های زیر پاسخ دهید:

-آیا رایانه در یک فضای عمومی از خانه قرار دارد؟

-چه وب‌سایت‌هایی برای بازدید کودکان شما مناسب هستند؟

-زمانی که برای آن صرف می‌کنند چقدر باید باشد؟

-زمانی که آنلاین هستند چه کاری باید انجام دهند؟

-چه کسانی اجازه دارند که با او در تعامل و ارتباط باشند؟

-اگر شما آن‌ها را کنترل نکنید، چه وقت بایستی کمک، راهنمایی و تأیید شما را طلب کنند؟

زمانی که شما به سؤال‌های بالا پاسخ دادید، شما می‌توانید صحبت با کودکان را آغاز کنید. برای این که تمرکز و حواس کودک را به خود جلب کنید، رایانه را خاموش کنید. بایستی برای آنان تشریح کنید که رایانه یک ابزار است و ضروری است که در زمان آنلاین شدن، ایمنی آن را حفظ کنید.

مطمئن شوید که این نکات را بیان خواهید کرد:

-بحث در مورد ویروس‌ها، جاسوس‌ابزارها و هکرها

-بحث در مورد این‌که شکارچیان کودکان چگونه توجّه آنان را برای صحبت کردن در باره‌ی خودشان جلب می‌کنند.

-تشریح کنید که به دلیل این که رایانه یک در باز به سمت اطّلاعات مهم شخصی شماست، ضروری است که در هنگام آنلاین شدن از امنیت لازم برخوردار باشید.

-بحث در مورد این که سرقت هویّت به چه نحو اتّفاق می‌افتد.

-بحث در مورد این واقعیت که شما یا یک خبره‌ی رایانه (در صورتی که شما خبره نباشید) می‌توانید هرگونه اتّفاقی را که بر روی کامپیوتر می‌افتد، ردگیری کنید.

-صحبت در باره‌ی این که چگونه مجرمین می‌توانند کنترل رایانه‌ی شما را به دست بگیرند به نحوی که شما مجبور باشید، یک رایانه‌ی تازه بخرید.

ب) کمک‌خواستن در زمانی که اتّفاقات ناراحت‌کننده‌ای در فضای آنلاین رخ می‌دهد.

به کودکان خود تاکید کنید که اگر در طول چت کردن خود پیام نامربوط یا نامناسبی را دریافت می‌کنند، به شما اطّلاع دهند و شما نیز در مقابل آن‌ها را دعوا نمی‌کنید و دسترسی آن‌ها به اینترنت را نیز قطع نخواهید کرد .کودکان را توجیه کنید که شما می‌دانید که آن‌ها قادر به کنترل کردن آن‌چه که دیگران می‌گویند نیستند و شما آن‌ها را به این دلیل سرزنش نخواهید کرد.

همچنین، مطمئن شوید که کودکان شما در فضای اینترنت نسبت به کودکان دیگر قلدری نمی‌کنند یا مورد قلدری قرار نمی‌گیرند. زمانی که کودکان مدرسه را ترک می‌کنند، لزوماً همکلاسی‌ها و درگیری‌هایی که با آن‌ها دارند را ترک نمی‌کنند. آن‌ها با رایانه، نامه و تلفن‌های همراه با هم می‌توانند در ارتباط باشند و ممکن است از این تکنولوژی‌ها برای اذیت و آزار یکدیگر، قلدری کردن و آسیب رساندن به دیگران استفاده کنند.

ج) چگونه جلوی کاربران را بگیریم و مسائل را گزارش کنیم

شما می‌توانید تمام مکالمات صورت گرفته را در یک واژه پرداز کپی و جایگذاری کنید. بسیاری از نرم‌افزارهای گفتگوی آنلاین به شما اجازه می‌دهند تا با راست

کلیک کردن بر روی نام کاربران در لیست دوستان‌تان آن‌ها را «مسدود» یا از آن‌ها «صرف‌نظر» کنید. اگر کودک شما در معرض یک تعرّض آنلاین قرار گرفته است، یک کپی از سابقه‌ی مکالمات را به مدیر اطاق گفتگو ارسال یا مدیر سایت ارسال کنید. شما می‌توانید اطّلاعات تماس را از بخش «کمک» یا بخش »گزارش‌دهی» برنامه دریافت کنید .

الفبای امنیت آنلاین برای نوجوانان ۱۳ تا ۱۹ ساله

الف) با نوجوانان خود صحبت کنید

همان‌طور که شما دوست دارید امنیت عبور و مرور را پیش از آن‌که آنان شروع به رانندگی کنند، به نوجوانان خود بیاموزید، همچنین باید در رابطه با امنیت اینترنت نیز، پیش از آن‌که به آنان اجازه دهید بدون نظارت شما در اینترنت گشت بزنند، آنان را آموزش دهید.

یک فرق عمده بین رانندگی و استفاده از اینترنت آن است که «قوانین عبور و مرور» واقعی در اینترنت وجود ندارد. به همین خاطر اینترنت را تبدیل به یک وسیله‌ی نقلیه قدرت‌مند و البته خطرناک تبدیل کرده‌است. بنابر این، برای کاستن از خطرات و آسیب‌های رایانه، شما بایستی قوانینی را تعریف کنید و به اجرا بگذارید. در این‌جا هدف نهایی، تربیت و آموزش حسّ مشترک نوجوانان برای درک روشن و شفّاف خطرات آنلاین است.

با نوجوانان خود صحبت کنید که چرا ضروری است که در فضای آنلاین ایمن باشند .مطمئن شوید که در طیّ این صحبت‌ها موارد ذیل را ذکر می‌کنید:

-بحث در باره‌ی ویروس‌ها، جاسوس‌افزارها و هکرها و اقداماتی که انجام می‌دهند.

-بحث در رابطه با شکارچی‌های آنلاین که دوست دارند توجّه نوجوانان برای صحبت‌کردن درباره‌ی خودشان جلب کنند.

-تشریح کنید که به دلیل این که رایانه یک در باز به سمت اطّلاعات مهم شخصی شماست، ضروری است که در هنگام آنلاین شدن از امنیت لازم برخوردار باشید.

-بحث درباره‌ی این که سرقت هویّت چگونه اتّفاق می‌افتد.

-بحث در مورد این واقعیت که شما یا یک خبره‌ی رایانه (در صورتی که شما خبره نباشید) می‌توانید هرگونه اتّفاقی را که بر روی کامپیوتر می‌افتد، ردگیری کنید.

-صحبت در باره‌ی این که چگونه مجرمین می‌توانند کنترل رایانه‌ی شما را به دست بگیرند به نحوی که شما مجبور باشید، یک رایانه‌ی تازه بخرید.

ب) به نوجوانان خود گوشزد کنید افرادی که به صورت آنلاین در اینترنت ملاقات می‌کنند، غریبه هستند.

مهم نیست که غالباً چگونه با آن‌ها چت می‌کنند و مهم نیست که آن‌ها فکر می‌کنند که مخاطب خود را می‌شناسند، مهم این است که بدانند افرادی که به صورت آنلاین آن‌ها را ملاقات می‌کنند، غریبه هستند. مردم راجع به این که حقیقتاً که هستند دروغ می‌گویند و «دوست» تازه‌ی نوجوان شما ممکن است در واقعیت یک مرد چهل ساله باشد که خود را در سنّ و سال نوجوان شما جا زده است.

ج) پروفایل نوجوان خود را در سایت‌های شبکه‌های اجتماعی چک کنید

مطمئن شوید که نوجوانان شما، اطّلاعات زیادی درباره خودشان را در سایت‌های مثل فیس‌بوک، مای‌اسپیس و سایر سایت‌های شبکه‌های اجتماعی، ارسال نکنند .مطمئن شوید عکس‌هایی که در سایت ارسال می‌کنند، برانگیزاننده نباشد. به آن‌ها یادآوری کنید که اگر به دام شکارچی‌های اینترنتی بیفتند، عواقب و سوء پیشینه‌ی آن ممکن است خانواده و دوستان را شرمسار کرده، در پذیرش آنان در دانشگاه یا در استخدام آنان در سازمان‌ها و شرکت‌ها تاثیر داشته باشد.

چطور امنیت خانواده را در اینترنت حفظ کنیم؟

میلیون‌ها خانواده هر روزه از اینترنت برای یادگیری، تحقیق، خرید، انجام امور بانکی، به اشتراک‌گذاری تصاویر، بازی، دانلود فیلم و موسیقی، ارتباط با دوستان، ملاقات افراد جدید و ... استفاده می‌کنند که برای حفظ امنیت در این محیط دانستن اصول اولیه محافظت ضروری است.

با ورود اعضای خانواده به دنیای آنلاین، صرفنظر از سن آنها باید آموزش‌هایی در مورد امنیت فضای سایبر به آنها داده شود چرا که آمارها نشان می‌دهد هکرها هر ۳۹ ثانیه از طریق اینترنت به کامپیوترهای افراد حمله می‌کنند. همچنین بیش از دویست هزار ویروس کامپیوتری تاکنون شناخته شده که این تعداد هر روز در حال افزایش است و یک سوم سایت‌های اینترنتی نیز در تسخیر مسائل غیراخلاقی است.

طبق بررسی‌های صورت گرفته جرائم اینترنتی از سال ۲۰۰۷ تا ۲۰۰۸ نیز حدود ۳۳ درصد افزایش داشته‌اند و در سال ۲۰۰۸ حدود ۹.۹ میلیون آمریکایی قربانی سرقت یا جعل هویت قرار گرفته‌اند.

اما در کشور ما با توجه به جدید بودن بحث استفاده از ابزار الکترونیکی برای امور روزمره و عدم شناخت کافی از جرائم رایانه‌ای، اهمیت دانستن اصول اولیه محافظت در فضای سایبر امری است که به شدت احساس می شود.

گفته شده است که به دلیل نبود آموزش‌های مدون به کاربران رایانه ای حدود ۵۰ تا ۶۰ درصد سیستم ها در ایران در خطر جاسوسی الکترونیک هستند.

ضرورت حفظ امنیت اعضای خانواده در اینترنت

شرکت‌هایی که در زمینه تولید ابزارهای فیلترینگ برای کنترل دسترسی کودکان به اینترنت فعالیت می‌کند، در گزارش‌های خود اعلام کرده‌اند که بیش از یک سوم اینترنت را سایت‌های غیراخلاقی تشکیل می‌دهند که می‌توانند آسیب‌های فراوانی به کودکان و حتی بزرگسالان وارد کنند.

مزایا و معایب اینترنت برای کودکان

بر اساس نتایج حاصل از این مطالعات مشخص شده که از کل اینترنت بیش از ۳۷ درصد سایت‌ها با موضوعات غیراخلاقی فعالیت می‌کنند. تعداد سایت‌های اینترنتی ارائه دهنده خدمات بازی‌های آنلاین طی یک سال گذشته ۲۱۲ درصد افزایش یافته و سایت‌های حاوی بخش‌های خشونت‌آمیز ۱۰ درصد بیشتر شده که این امر هشداری برای استفاده بدون کنترل کودکان از اینترنت است.

بر این اساس و با وجودی که آگاهی کودکان و نوجوانان برای دسترسی آسان به این سایت‌ها روز به روز افزایش می‌یابد، لزوم دقت و کنترل خانواده‌ها برای کاهش ورود به این سایت‌های اینترنتی توسط کودکان ضروری خواهد بود.

توصیه‌هایی برای جلوگیری از تهدیدات سایبری

از آنجایی که دانستن اصول اولیه محافظت در فضای سایبر امری ضروری به نظر می‌رسد رعایت نکاتی در اینباره به تمامی خانواده‌ها توصیه می‌شود:

۱-به محل قرار دادن کامپیوتر در خانه دقت کنیم

در خانه‌ای که کودکان و نوجوانان در آن زندگی می‌کنند، محل قرار گرفتن کامپیوتر خانواده بسیار مهم است. بنابراین بهتر است که کامپیوتر خانوادگی در محلی از خانه قرارگیرد که محل رفت و آمد زیاد اعضای خانواده باشد و تعداد ساعاتی که بچه‌ها با این کامپیوتر کار می‌کنند نیز محدود باشد. بهتر است والدین اطمینان حاصل کنند که سیستمشان دارای نرم‌افزار امنیتی حاوی ابزارهای کنترلی والدین باشد.

۲-کارکردن تیمی برای مشخص کردن محدودیت‌ها

خانواده‌ها باید دقیقا در مورد اینکه چه چیزهایی مناسب یا نامناسب است تصمیم‌گیری کرده و در این کار فرزندان خود را مشارکت دهند. برای این کار باید مواردی چون انواع وب سایت‌های مناسب، اتاق های چت و روم هایی که برای مشارکت مناسب هستند توجه کنند.

همچنین از اتاق‌های چت نظارت شده استفاده شود و این اطمینان حاصل شود که به غیر از این موارد فرزندان از دیگر اتاق‌های چت استفاده نکنند چرا که این اتاق‌های چت می‌توانند حاوی موضوعات نامناسبی برای افراد جوان باشند. خانواده‌ها همچنین باید انواع چیزهایی که فرزندان می‌توانند به صورت آنلاین در مورد آن بحث کنند را مشخص کنند.

۳- در خانه در مورد قوانین کامپیوتر خانگی توافق شود

برای توافق بر سر استفاده از کامپیوتر خانگی بهتر است که برخی قوانین در این رابطه وضع شود. هرگز کلمه عبور خود را فاش نکنید. هرگز شماره تلفن یا آدرس خود را افشا نکنید. هرگز اطلاعاتی را که هویت شما را آشکار می کند ارسال نکنید و هرگز تصاویر نامناسب یا تصاویری که هویت شما را افشا می کند ارسال نکنید.

همچنین براساس این قوانین هیچ گونه اطلاعاتی را با غریبه هایی که به صورت آنلاین ملاقات می‌کنید به اشتراک نگذارید. هرگز با غریبه‌هایی که به صورت آنلاین آشنا شده اید، قرار ملاقات نگذارید و هرگز ضمایم ایمیل‌های ارسال شده از طرف غریبه‌ها را باز نکنید. بهتر است این قوانین به اطلاع همه اعضای خانواده رسانده شود.

۴-نصب نرم افزارهای امنیتی روی سیستم

خانواده‌ها باید اطمینان حاصل کنند که نرم افزار امنیتی مستحکمی دارند که سیستمشان را در برابر ویروس‌ها، هکرها و جاسوس افزارها محافظت می‌کند. این نرم افزار امنیتی همچنین باید محتوا، تصاویر و وب سایت‌های خطرناک را فیلتر کند. این نرم افزار باید مرتب به روزرسانی شود چرا که هر روزه تهدیدات جدیدی متولد می‌شوند که به روزرسانی خودکار نرم افزارهای امنیتی بسیار می‌تواند در این زمینه موثر واقع شود.

۵-از ابزارهای کنترلی و نظارتی والدین استفاده شود

تمامی نرم افزارهای امنیتی مهم و پرکاربرد، ابزارهای نظارتی و کنترلی ویژه والدین ارائه می‌دهند. برای یاد گرفتن نحوه کار با این ابزارها باید زمان گذاشت و از گزینه‌هایی که موضوعات و محتوای نامناسب را فیلتر و مسدود می‌کنند استفاده کرد.

برخی تولید کنندگان نرم افزارهای امنیتی علاوه بر قرار دادن ویژگی های نظارتی در این نرم افزارها، نرم افزار خاصی نیز ویژه نظارت والدین بر فعالیت‌های آنلاین فرزندان خود عرضه کرده اند. برای مثال شورای عالی اطلاع رسانی نیز نرم افزار فیلترینگ خانگی را عرضه کرده که به صورت رایگان از طریق پرتال این شورا قابل دسترسی است.

این نرم افزارها فرزندان خانواده را از دسترسی به محتوای نامناسب، خطرات شبکه‌های اجتماعی، افراد غریبه و سایر تهدیدات آنلاین بر حذر می‌دارند. البته این ابزارها دارای محدودیت‌های خاص خود نیز هستند و بهتر است والدین خود، شخصا به نظارت بر کار فرزندانشان در اینترنت بپردازند.

۶- افراد آنلاین، غریبه هستند

هر کسی که آنلاین می‌شود باید این نکته را به خاطر بسپارد که صرفنظر از اینکه دوستان آنلاین را چند دفعه به صورت آنلاین ملاقات کرده و صرف نظر از اینکه چه مدت با این افراد چت کرده و صرف نظر از اینکه چقدر آنها را می‌شناسد، افرادی که به صورت آنلاین ملاقات کرده افرادی غریبه هستند و دروغ گفتن در مورد هویت شخصی برای فرد آنلاین کاری بسیار ساده است. همچنین کودکان و نوجوانان باید بدانند که فردی که وانمود می کند هم سن آنهاست، می تواند ۴۰ ساله باشد.

با وجودی که وب سایت‌های شبکه‌های اجتماعی می تواند راه ایده آلی برای ملاقات افراد جدید به صورت آنلاین باشد به خانواده‌ها توصیه می‌شود وارد این سایت‌ها شده و پروفایل فرزندان خود را چک کنند تا اطمینان حاصل کنند که مکالمات نامناسبی رخ نداده باشد و تصاویر غیرقابل قبولی ارسال نشده باشد.

والدین باید مکالمات آنلاین فرزندان خود را بررسی کنند تا مطمئن شوند در معرض خطر افراد خطرناک قرار ندارند.

۷-انتخاب کلمات عبور قوی

برای ایجاد کلمات عبور قوی که به راحتی کشف نشوند، باید کلمه عبور شما حداقل ۸ کاراکتر داشته باشد و ترکیبی از حروف، ارقام و نشانه‌ها باشد. کلمات عبور باید در فواصل زمانی معین تغییر کنند تا احتمال سوء استفاده از یک کلمه عبور در طول زمان کاهش یابد. همچنین رعایت این نکته نیز الزامی است که کلمه عبور خود را با دیگران به اشتراک نگذارید.

۸- چک کردن نرم افزار امنیتی سیستم

کاربران باید نرم افزار امنیتی خود را باز کرده و اطمینان حاصل کنند که سه ویژگی آنتی ویروس، ابزار ضدجاسوسی و فایروال را دارا است. این هسته‌های محافظتی باید با ابزار ضد هرزنامه و نرم افزار جستجوی امن نیز تقویت شوند.

ایده بسیار خوبی است که خانواده ها یک مجموعه امنیتی برروی کامپیوتر خانوادگی خود داشته باشند که شامل ابزارهای کنترلی والدین و ابزارهای جلوگیری از سرقت هویت نیز باشد.

۹-با کودکان خود صحبت کنیم

والدین باید مراقب باشند که فرزندانشان با افراد هم سن و سال خود در اینترنت ارتباط برقرار نکنند. به همین علت به والدین توصیه می شود که برای فرزندان کوچک خود در مورد کامپیوتر، اینترنت و اهمیت حفظ امنیت در اینترنت توضیح داده و نحوه نفوذ هکرها به کامپیوتر آنها و از کار انداختن سیستم را برای آنها شرح دهند.

والدین باید برای فرزندان در مورد اهمیت عدم افشای اطلاعات شخصی در اینترنت کاملا توضیح دهند و بگویند که نباید در مورد محل زندگی یا مدرسه خود برای دیگران توضیح دهند.

از کودکانمان بخواهیم که فرمهای آنلاین را بدون حضور ما پر نکنند و برای جستجو، موتورهای جستجوی ویژه کودکان مانند Yahoo! Kids را به آنها معرفی کنیم. برای فرزندان بزرگتر نیز در مورد ویروس‌ها، جاسوس افزارها و هکرها و نحوه کار آنها شرح داده و به آنها بگوییم که سرقت هویت چگونه اتفاق می‌افتد. برای آنها توضیح دهیم که هر اتفاقی بر روی کامپیوتر می‌افتد توسط شما قابل بررسی و ردیابی است. به آنها اطمینان دهیم که در صورت وقوع هر اتفاقی به آنها کمک خواهیم کرد و نحوه مسدود کردن کاربران مزاحم را به آنها یاد دهیم.

۱۰- آگاهی‌مان را افزایش دهیم

هر چه بیشتر بدانیم از امنیت بیشتری برخوردار خواهیم بود. برای این منظور به اخبار امنیتی و به روز رسانی‌های امنیتی توجه کرده و مقالات ساده امنیتی را مطالعه کنیم.

یک برنامه‌ی ۱۰ قدمی برای کمک به حفاظت از اعضای خانواده شما

مرحله یک: محل قرارگیری رایانه

در خانه‌ای که کودکان در آن حضور دارند، جایی که رایانه‌ی خانواده را در آن قرار می‌دهید، یکی از مهم‌ترین تصمیماتی است که می‌توانید اتّخاذ کنید. ما توصیه می‌کنیم که رایانه را در یک فضای پر تردّد از محیط خانه قرار دهید و تعداد ساعت‌هایی را که کودکان صرف آن می‌کنند، محدود کنید. مطمئن شوید که نرم‌افزارهای امنیتی رایانه‌ای که شامل ابزارهای نظارت و کنترل والدین هم هستند؛ نظیر محصولاتی که در مک‌آفی می‌توانید بیابید {آنتی‌ویروس‌ها و نرم‌افزارهای امنیت اینترنت (Internet Security)} را در اختیار دارید.

مرحله دو: مثل یک تیم کار کنید

برای تعیین حدود و مرزها

دقیقاً تصمیم بگیرید که چیزی درست است و چه چیزی درست نیست؛ در رابطه با:

-درباره‌ی انواع وب‌سایت‌هایی که برای بازدید مناسب‌اند.

-درباره‌ی اطاق‌های گفتگو و انجمن‌هایی که برای شرکت کردن مناسب هستند:

oتنها از اطاق‌های گفتگویی که بر آن‌ها نظارت می‌شود، استفاده گردد.

oمطمئن شوید که از دسترسی فرزندانتان به اطاق‌های گفتگوی بزرگسالان که با نماد alt. مشخّص می‌شوند جلوگیری می‌شود. این اطاق‌های گفتگو بر روی موضوعات جایگزینی تمرکز می‌کنند که ممکن است برای افراد کم سنّ و سال مناسب نباشند

-درباره‌ی انواع موضوعاتی که کودکان می‌توانند به صورت آنلاین راجع به آن‌ها بحث کنند و نوع بیانی که نامناسب تلقّی می‌شود.

مرحله‌ی سوّم: با هم بر اساس توافق

قوانین رایانه‌ی خانوادگی

ما موارد ذیل را توصیه می‌کنیم

-هرگز با نام کاربری ای که هویّت واقعی را نشان می‌دهند یا تحریک آمیزند به رایانه وارد نشوید.

-هرگز کلمه‌ی عبور خود را به نمایش نگذارید.

-هرگز شماره‌های تلفن یا آدرس‌های خود را به نمایش نگذارید.

-هرگز اطّلاعاتی را که نشان‌دهنده‌ی هویّت شماست، ارسال نکنید.

-هرگز تصاویر نامناسب یا چیزهایی را که هویت شما را به نمایش می‌گذارند ارسال نکنید. (برای مثال: عکس‌هایی که در آن بر روی لباس شما نام مدرسه یا شهر شما نوشته شده‌است)

-هرگز هیچ‌گونه اطّلاعاتی را با غریبه‌هایی که آن‌ها را به صورت آنلاین می‌بینید، به اشتراک نگذارید.

-هرگز به صورت چهره به چهره با غریبه‌هایی که آن‌ها را به صورت آنلاین می‌بینید، ملاقات نکنید.

-هرگز فایل‌های رایانه‌ای متصّل شده به ایمیل‌هایی که از غریبه‌ها دریافت می‌کنید باز نکنید.

زمانی که شما این قوانین را وضع کردید، یک پوستر از آن‌ها درست کنید و آن را در کنار کامپیوتر قرار دهید.

مرحله‌ی چهارم: یک قرارداد امضا کنید

برای رفتار مناسب آنلاین

یک قرارداد بنویسید ؛ که در آن درک روشنی در میان اعضای خانواده در استفاده مناسب از رایانه و رفتارهای آنلاین وجود دارد.

تعهّدنامه امنیت آنلاین

از این رو که رایانه و اینترنت امتیازی است که من نمی‌خواهم آن را از دست دهم،

-هر زمانی که آنلاین باشم، به صورت کاملاً ایمن به گشت و گذار در اینترنت، جستجو، کار، بازی و چت خواهم پرداخت.

-من از تمامی قوانینی که بر سر آن توافق کرده‌ایم پیروی خواهم کرد.

-من نام واقعی، شماره‌ی تلفن، آدرس و کلمه‌ی عبورم را برای دوستان آنلاین به نمایش نخواهم گذاشت.

-من هرگز به صورت شخصی با افراد آنلاین ملاقات نخواهم کرد.

-اگر خود را در موقعیتی بیابم که در آن ناایمن یا ناراحت باشم، قول می‌دهم که شما را آگاه کنم. (پدر و مادرم، سرپرست یا معلّم‌ام) می‌دانم که شما می‌توانید به من کمک کنید.

-من به این تعهّدنامه وفادارم و تبعات تصمیمات خود را می‌پذیرم.

امضای کودک.....

-به عنوان پدر و مادر/ سرپرست/ معلّم، من قول می‌دهم، زمانی که تو نیاز به من به عنوان یک راهنما داری در دسترس تو باشم و به تو برای حلّ هر مشکلی که قادر به رفع کردن آن باشم، کمک کنم.

امضای پدر و مادر/ سرپرست/ معلّم

مرحله‌ی پنجم: نرم‌افزارهای امنیتی را نصب کنید

مطمئن شوید که شما نرم‌افزارهای امنیتی قابل اعتماد که رایانه‌ی شما را در برابر ویروس‌ها، هکرها و جاسوس‌افزارها محافظت می‌کند، در اختیار دارید . همچنین آن بایستی محتواها، عکس‌ها و وب‌سایت‌های توهین‌آمیز را فیلتر کند .این نرم‌افزار باید به صورت مداوم به روزرسانی گردد چنان‌که تهدیدهای جدید به صورت روزانه به وجود می‌آیند. ایده‌آل است که این نرم‌افزارها مثل نرم‌افزارهای «نصب کن و رها کن مک‌آفی» به صورت اتوماتیک به روزرسانی گردند. این بهترین انتخاب است.

مرحله‌ی ششم: از نرم‌افزارهای نظارت والدین استفاده کنید

تمامی عرضه‌کنندگان عمده‌ی نرم‌افزارهای امنیتی، نرم‌افزارهای نظارت والدین را ارائه می‌کنند. مطمئن باشید که آن‌ها را فعّال کرده‌اید. اگر شما از نرم‌افزارهای رایگان یا از نرم‌افزارهایی که نظارت والدین ندارند استفاده می‌کنید، نرم‌افزاری را برای سفارش دادن در نظر بگیرید که شامل نظارت والدین نیز می‌شود. زمانی را صرف کنید تا یاد بگیرید که این کنترل‌ها چگونه کار می‌کنند و از گزینه‌هایی که موارد نامناسب را فیلتر یا مسدود می‌کنند استفاده کنید. البته، این ابزارها محدودیت‌های خاصّ خود را دارند. هیچ چیز نمی‌تواند جای پدر و مادر مسؤول و پاسخگویی را بگیرد که فرزندان خود را در زمانی که آنلاین هستند مراقبت می‌کند.

مرحله‌ی هفتم: به خانواده‌ی خود یادآوری کنید که افراد آنلاین غریبه هستند.

هرکسی که آنلاین می‌شود باید بداند که:

مهم نیست که چگونه اغلب شما با دوستان آنلاین‌تان چت می‌کنید، مهم نیست که چقدر چت می‌کنید و مهم نیست که شما چقدر فکر می‌کنید که آن‌ها را می‌شناسید. مهم این است که افرادی که شما به صورت آنلاین آن‌ها را ملاقات می‌کنید غریبه هستند. خیلی ساده است که در زمانی که شما آنلاین هستید، به شما دروغ بگویند و خود را کس دیگری جا بزنند. خصوصاً کودکان لازم است بدانند که ممکن است یک «دوست» جدید، در واقعیت یک مرد چهل‌ساله باشد تا یک نفر هم سنّ و سال خودشان.

شبکه‌های اجتماعی مثل مای‌اسپیس و فیس‌بوک یک راه حلّ ایده‌آل برای آشنایی با افراد جدید هستند. بنابراین، پدر و مادر بایستی این سایت‌ها مشاهده کرده و پروفایل فرزندان خود را بازرسی کنند تا مطمئن شوند که صحبت‌های نامناسب جایی در آن نداشته باشند و عکس‌های غیرقابل قبول ارسال نگردند. پدر و مادر بایستی مکالمات و چت‌های اینترنتی فرزندان خود را نظارت کنند تا مطمئن شوند که آنان توسّط شکارچیان آنلاین تعقیب نمی‌شوند.

مرحله‌ی هشتم: یک کلمه‌ی عبور قوی بسازید

برای ساختن رمز عبوری که شکستن آن سخت باشید، از حدّاقل هشت کاراکتر که ترکیبی از حروف، اعداد و سمبل‌هاست، استفاده کنید. رمز عبور باید به صورت دوره‌ای تعویض شود تا احتمال به خطر افتادن یک رمز عبور در طول زمان کاهش یابد.

تکنیک‌های ساخت رمز عبورهای قوی عبارتند از:

-استفاده از شماره شاسی خودرو«GR8wayy2B» :

-استفاده از چند کلمه‌ی کوچک به همراه علائم نگارشی«betty,boop$car» :

-قراردادن علائم نگارشی در وسط کلمه«Roos%velt» :

-استفاده از یک روش غیر معمول قراردادی در یک کلمه«ppcrnbll» :

-استفاده از حرف اوّل هر کلمه در یک عبارت به همراه یک عدد تصادفی«hard to crack this password=htc5tp» :

-کلمه‌ی عبور خود را به اشتراک نگذارید!

مرحله‌ی نهم: نرم‌افزارهای امنیتی خود را کنترل کنید

هر از چندی، نرم‌افزارهای امنیتی خود را باز کنید و کنترل نمایید که رایانه‌ی شما با این سه محافظ اصلی، محافظت می‌شود: ضد ویروس، ضد جاسوس‌افزار و دیواره‌ی آتش (فایروال)

به این محافظ‌های اصلی، نرم‌افزارهایی مثل ضد اسپم و نرم‌افزارهای جستجوی امن مثل مک آفی سایت ادوایزر که دارای آنتی فیشینگ و رتبه‌بندی ایمنی هم هستند بایستی افزوده شود. این ایده‌ی خوبی برای خانواده است که مجموعه‌ای از نرم‌افزارهای حفاظتی را بر روی رایانه‌شان داشته باشند که همچنین شامل نرم‌افزارهای نظارت والدین و ابزارهای جلوگیری از سرقت هویّت است.

مرحله‌ی دهم: همیشه آگاه باشید

هر چقدر بیشتر بدانید، بیشتر در امنیت خواهید بود.

آموزش اصول امنیتی آنلاین برای کودکان

گرچه امروزه یک شکاف عمیقی بین والدین و فرزندان از لحاظ اطلاعات کامپیوتری و اینترنتی وجود دارد، اما والدین با رعایت چند نکته ساده و آموزش آن‌ها به فرزندان می‌توانند تا حدود زیادی فرزندان خود را از خطرات ناشی از فضای مجازی به دور نگهدارند. در اینجا برخی از آموزش‌های اساسی که والدین می‌توانند به فرزندان خود ارائه دهند ذکر می‌شود.

تشویق بچه‌ها برای حفظ رمز عبور خود:

با توجه به مطالعه‌ای که توسط گروه Teenangels صورت گرفته ۷۵ درصد از کودکان ۹-۸ ساله و ۶۶ درصد از دختران ۱۲-۷ ساله رمز عبور خود را با شخص دیگری به اشتراک گذاشته‌اند.

اولین قانون امنیت اینترنت این است که :کلمه عبور خود را مخفی نگهدارید. تشویق کودکان به حفظ رمز عبور خود تا حدود بسیار زیاد از اطلاعات شخصی آنها محافظت می کند.

در زیر برخی از قوانین بسیار مهمی که بچه‌ها باید بدانند ارائه شده است:

۱. آیا رمز عبور خود را از دیگران مخفی نموده‌اند؟ حتی از دوستان خود.

۲. حفاظت از رمزهای عبور ثبت شده. باید از کودکان خود بخواهیم رمزهای عبور خود را در کیف مدرسه یا کیف پول خود نگه ندارند یا حتی الامکان آنها را به طور کامل مخفی کنند.

۳. هرگز رمز عبور خود را با یک درخواست از طریق ای‌میل یا پیام کوتاه به کسی ارسال نکنند. این موضوع حتی شامل درخواست از وب‌سایت‌های مورد اعتماد نیز می‌باشد چون افراد کلاه‌بردار معمولا با استفاده از نام‌ها و آرم‌های جعلی (فیشینگ) برای دسترسی به اطلاعات شخصی اقدام می‌کنند.

۴. از کلمه عبور یکسان برای حساب‌های کاربری خود در جاهای عمومی مثل کتابخانه مدرسه، کافی‌نت ها یا سایت کامپیوتر استفاده نکنند.

۵. حتی الامکان دسترسی بچه‌های خود را به شبکه‌های اجتماعی محدود کنید چون ممکن است به راحتی در معرض خطرهایی نظیر کلاهبرداری‌های فیشینگ، فشارهای آنلاین (تهدیدات آنلاین) و شکارچیان اینترنتی قرار بگیرند.

۶. در مورد تجارب خود با فرزندان صحبت کنید چون ممکن است فرزندان شما با هر چیز در اینترنت روبرو شوند و براحتی دچار اضطراب و ناراحتی شوند. آنها باید آموزش ببینند که به راحتی به هر پیامی جواب مثبت ندهند (ok)و به آنها آموزش دهید که با شما مشورت کنند.

۷. به فرزندان خود آموزش دهید که با افراد غریبه در اینترنت هم کلام نشوند و در عوض با افرادی که از نظر شما قابل تأیید هستند در ارتباط باشند.

۸. به فرزندان آموزش دهید که از نام کامل خود استفاده نکنند و به جای آن با یک نام مستعار مناسب در فضای مجازی ظاهر شوند و از انتخاب نام های نامناسب که ممکن است هر فردی را جذب کند اجتناب کنند.

۹. از اطلاعات شخصی و پروفایل فرزندان خود به خوبی محافظت کنید به این دلیل که با استفاده از این اطلاعات به راحتی گروه های مختلف که ممکن است افراد ناشناس زیادی در آن باشند به طرف فرزندانتان کشیده شوند.

۱۰. مراقب باشید فرزندان اطلاعات شخصی خود همانند نام مدرسه، محل زندگی، نام باشگاه و ... را در فضای مجازی به اشتراک نگذارند.

۱۱. به فرزندان خود بگویید از قرار دادن عکس‌های خود و دوستان که دارای نشانه‌هایی از محل زندگی یا مدرسه خود هستند در فضای مجازی به شدت خودداری نمایند.

۱۲. به فرزندان خود آموزش دهید که اگر در فضای مجازی تهدید شدند بهترین کار مشورت با پدر، مادر یا معلمین خود می‌باشد.

آموزش نکاتی به کودکان در مورد شبکه های اجتماعی

به کودکانمان چگونگی امنیت در شبکه های اجتماعی را آموزش دهیم:

همانطور که می دانید ، شبکه های اجتماعی به سرعت در حال رشد و توسعه می باشند و در ۲ سال اخیر در کشورمان نیز در فضای اینترنت در تطابق با آداب و رسوم ایرانی و اسلامی این شبکه ها شکل گرفته و در حال رشد هستند. امروزه عضویت در شبکه های اجتماعی در کودکان نیز فراگیر شده است. ما به شما راههایی را پیشنهاد می کنیم تا بتوانید از فرزندانتان در فضای مجازی محافظت کنید.

در رابطه با آن والدینی که اطلاعات کامپیوتری و اینترنتی فرزندانشان نسبت به آنها بیشتر است، باید بدانند کودکان به اندازهٔ کافی بزرگ نیستند تا همهٔ رفتار و موارد گوناگونی که در اینترنت وجود دارد را درک کنند و حتی در مواردی در اینترنت مورد تهدید قرار می گیرند، پس والدین می بایست روی کامپیوتر فرزندانشان در منزل نظارتی دقیق داشته باشند.

ما رعایت نکات زیر را به والدینی که می خواهند فرزندانشان هنگام ورود به اینترنت امنیت داشته باشند توصیه می کنیم.

•تفاوت بین اشتراک گذاری اطلاعات و فاش کردن اطلاعات را به کودکان بیاموزیم. مثلاً وقتی در اینترنت صحبت از به اشتراک گذاری عکس، عقاید، تجربه ها و .... است به کودکان بیاموزیم هرگز اطلاعات شخصی، شماره تماس، آدرس، شماره حساب بانکی، پس ورد و .... را به اشتراک نگذارند. همچنین با آنها در مورد اینکه اگر عکس یا اطلاعاتی را در اینترنت به اشتراک گذارند، اگر چه می توان بعدها آن را حذف کرد اما امکان خطر حتی در همان زمان کوتاه وجود دارد، و نمی توان اثرات آن را به کلی از بین برد، صحبت کنید.

•به کودکانمان آموزش دهیم هرگز با غریبه ها در محیط مجازی صحبت نکنند حتی اگر در حین صحبت کردن بتوانند آنها را ببینند : گفتگو با فرد غریبهٔ آنلاین، خطرناک و مضر است ، رابطه ای ممکن است بین آنها به وجود آید و آن فرد غریبه این رابطه را تا زمانی که فرزند شما به او اعتماد پیدا کند، ادامه ، و این موضوع می تواند موجب سوء استفاده از او گردد.

•به فرزندانمان آموزش دهیم تا دسترسی به اطلاعات پروفایل خود را برای همه جز افراد نزدیک مورد اعتماد و امن خود، محدود کنند. تنظیمات مستمرانه، حریم خصوصی وب‌سایت ، به کاربران این اجازه را می دهد تا انتخاب کنند اطلاعاتشان را با چه کسانی در میان گذارند .

•همیشه ارتباط دوستانهٔ خود با فرزندانتان را حفظ کنید تا آنها بدانند شما همیشه آمادهٔ صحبت با آنها در رابطه با هر مشکل یا مسأله ای که برای آنها در فضای مجازی رخ می دهد، هستید.

•هنگام استفادهٔ آنها از اینترنت، با آنها همراه شوید و برای خود در وب‌سایت هایی که فرزندتان در آن عضویت دارد، صفحه ای بسازید و عضو شوید. این کار به شما کمک می کند تا بتوانید بهتر با نحوه فعالیت و ارتباطات آن آشنا شوید و همچنین بتوانید تمام کارها و دوستان فرزندانتان را تحت نظر قرار دهید.

۷ نکته مهم برای حفاظت از کودکان در فضای مجازی

دانستن این که بچه ها در فضای مجازی از کجا سر در می آورند کار بسیار دشواری است. اما والدین باید به این نکته آگاه باشند که این مساله پر اهمیتی است هر چند کنترل این قضیه، کار زمان بری می باشد. دایره تجارت برتر ایالات متحده آمریکا، والدین را تشویق می کند بچه های خود را نسبت به مکان های نا امن آگاه کرده و به آنها علامت های مهم برای توقف فعالیت در دنیای مجازی را آموزش دهند.

بر اساس مطالعاتی که گروه نیلسن نورمن انجام داده است، بچه ها از سن ۹ سالگی به بعد در دنیای مجازی کنجکاوی بیشتری داشته و با تهدید های بیشتری مواجه هستند و به طور حتم بچه ها به اندازه ی پدر و مادرشان آگاهی ندارند و خیلی بیشتر از آنها در معرض خطر می باشند. بهترین راه برای محافظت از بچه های شما در محیط مجازی این است که راه های ارتباطی با آنها را باز نگه دارید و در مورد خطرات احتمالی با آنها صحبت کنید و به آنها بگویید هر وقت که احساس کردند در هفت موقعیت زیر قرار گرفتند باید فعالیت خود را متوقف کرده و به شما مراجعه کنند .

در زیر به این هفت موقعیت اشاره می کنیم :

۱.زمانی که از سایتی بازدید می کنند که اطلاعات مالی نظیر شماره حساب بانکی یا کارت اعتباری را می خواهد باید دقت کنند چون بعضی از سایت ها می خواهند از طریق فرزندان اطلاعات بانکی و مالی افراد را به دست آورده و آنها را وسیله ای برای دست یافتن به مقاصد شوم خود قرار دهند .

۲.زمانی که از سایتی بازدید می کنند که اطلاعاتی نظیر آدرس منزل، اسم و فامیل و آدرس پست الکترونیکی، شماره تلفن و شماره تأمین اجتماعی را می خواهند. باید مراقب باشند این اطلاعات برای شرکت هایی که می خواهند محصولات خود را برای آنها تبلیغ کنند و یا می خواهند هویت شخص را در محیط مجازی دزدیده و غارت کنند، بسیار با ارزش است. پس باید به این موضوع آگاه باشند و این اطلاعات را در دسترس این گونه سایت ها قرار ندهند .

۳.شخصی که آنها او را نمی شناسند و برای آنها تصاویر نامناسب می فرستد یا در ارتباط با آنها از زبانی نامناسب استفاده می کند یا می خواهد ملاقاتی داشته باشد خطرناک بوده و باید با احتیاط بیشتری با این گونه افراد برخورد کنند.

۴.زمانی که می خواهند تصاویر خود را در فضای مجازی ارسال کنند؛ ارسال تصاویر در فضای مجازی و به صورت آنلاین به ظاهر می تواند بی خطر باشد، اما اغلب یک کلید راهنمای مهم برای افراد شیاد می باشد.

۵.نسبت به سایت ها و شبکه های اجتماعی یا پیام الکترونیکی متعددی که دریافت می کنند هوشیارتر باشند، مزاحمت در فضای مجازی تنها یک شوخی بی ضرر نیست، به فرزندان خود بگویید در زمانی که تعداد این پیام ها زیاد شد حتماً شما را در جریان بگذارند.

۶.در شبکه های اجتماعی اگر از شخصی که نمی شناسند پیام دوستی دریافت کنند باید با هوشیاری بیشتری عمل کرده زیرا در فضای مجازی دوست شدن با شخصی که در دنیای واقعی او را نمی شناسند مانند باز کردن درب، برای انواع تهدیدها از جمله هکرها می باشد .

۷.در زمانی که فرزندان شما می خواهند خدمات رایگان از دنیای مجازی، مانند آهنگ های رایگان، زنگ تلفن همراه یا پیام های نوشتاری طنز رایگان دریافت نمایند، مطلع باشند که این گونه خدمات همواره هیچ هزینه ای نداشته اما اگر در مواردی بعضی سایت ها برای ارائه این گونه خدمات از آنها شماره حساب

خواست سریعاً شما را در جریان بگذارند تا صحت آن را بررسی نمایید .بهتر است فرزندان خود را در هر زمینه ای از جمله خطرات دنیای مجازی آموزش داده و آنها را از تهدیدات احتمالی در دنیای مجازی مصون بداریم .

سه نکته در قسمت ذیل پیشنهاد شده تا شما از منابع مالی خود در برابر کلاهبرداران و شرکت هایی که به اصول حرفه ای معتقد نیستند، حفاظت کنید.

از هر چیزی نسخه برداری کنید و همواره نسخه نهایی را بخوانید.

نسخه نهایی قراردادها و موافقت نامه ها با مشتری، همواره از مشاغل و شرکت های تجاری حمایت می کند و خلاصه ای کلی از شرایط قرارداد با مشتریان را مشخص می کند .اما یک مصرف کننده زیرک همیشه باید سوالاتی را مطرح کند و قراردادها را به دقت مطالعه نماید. در حالی که عدم مطالعه متون حقوقی پیچیده امری طبیعی است، مهم این است که مشتریان حقوق خود را بدانند و درک کنند. در مرحله امضای قرارداد، به شما پیشنهاد می کنیم نسخه نهایی را به دقت مطالعه کنید. حتی اگر می توانید نسخه نهایی را به خانه ببرید تا بتوانید آن را بیشتر و دقیق تر ارزیابی کنید. همچنین تنها به صحبت های مربوط به فروش اکتفا نکنید. تمامی قول و قرارهای شفاهی باید به صورت مکتوب باشند. و همیشه از دریافت رسید فروش اطمینان حاصل کنید .

همواره از مدارک مربوط به هویت شخصی و کیف جیبی خود محافظت کنید.

جنگ برای حفاظت از هویت شخصی همواره به معنای هوشیار بودن در فضای مجازی و دنیای واقعی است.
با انجام اقدامات زیر از هویت شخصی خود محافظت کنید:

-همواره اسناد مهمی را که حاوی اطلاعات مالی شخصی مانند شماره حساب بانکی، شماره کارت اعتباری و شماره تامین اجتماعی است، را خرد کنید).از بین ببرید)

-در فواصل زمانی نزدیک به هم، حساب های مالی خود را چک کنید تا به سرعت فعالیت های مشکوک را شناسایی کنید .

-اطمینان حاصل کنید که کامپیوتر (سیستم عامل) و نرم افزار ضد ویروس شما به روزرسانی شده است و در هنگام باز کردن ضمایم پیام های پست الکترونیکی (ایمیل) خود یا کلیک کردن بر روی لینک های موجود در ایمیل خیلی حساس باشید.

-خرید اینترنتی خود را فقط از سایت های مطمئن انجام دهید و همیشه قبل از آن که شماره کارت اعتباری خود را وارد کنید، اطمینان حاصل کنید که شرکت قابل اعتماد و مطمئن است.

هرگز پول خود را از طریق سیستم مخابراتی (ATM) برای شخصی که نمی شناسید، نفرستید .

بسیاری از کلاهبرداران با راضی کردن قربانیان برای ارسال پول از طریق سیستم مخابراتی، کلاهبرداری می کنند. نتایج ارسال پول می تواند بسیار متفاوت باشد و شامل خرید به صورتی پیچیده، پرداخت مبلغی برای بردن قمار و ...

–مشکل اساسی برای بیشتر قربانیان این است که برگشت پول آنها تقریباً غیر ممکن است. حتی اگر شما چکی را ارائه کرده باشید که فرضاً مبلغ ارسالی شما را پوشش می دهد، هیچ وقت برای کسی که شخصاً او را نمی شناسید، پول نفرستید.

۱۰ نکته برای حفظ امنیت کودکان در اینترنت

اینترنت می تواند مکانی گسترده برای کودکان باشد تا بیاموزند، سرگرم شوند، با دوستان مدرسه ای گپ بزنند، و با آسودگی خیال به مکاشفه بپردازند. اما درست همانند دنیای واقعی، وب هم می تواند برای کودکان خطرناک باشد. قبل از اینکه به کودکانتان اجازه دهید که بدون نظارت شما به اینترنت متصل شوند، یک سری از قوانین باید تعیین شوند.

اگر نمی دانید که از کجا آغاز کنید، در اینجا چندین ایده در مورد چیزهایی که باید با کودکانتان بحث کنید تا به آنها در مورد استفاده ایمن تر از اینترنت بیاموزید، آورده شده است:

۱- کودکانتان را تشویق کنید که تجارب اینترنتی خود را با شما سهیم شوند. همراه با کودکانتان از اینترنت لذت ببرید.

۲- به فرزندانتان بیاموزید که به غرایز خود اعتماد کنند. اگر در مورد چیزی احساس ناخوشایندی دارند، باید به شما درباره آن بگویند.

۳- اگر فرزندانتان به اتاق های گفتگو سر می زنند، از برنامه های پیام رسان فوری و بازی های ویدویی آنلاین استفاده می کنند، یا فعالیت های دیگری که به نامی برای مشخص کردن خودشان نیاز است، انجام می دهند، به آنها در انتخاب این نام کمک کنید و مطمئن شوید که این نام باعث افشاء هیچ اطلاعات شخصی درموردشان نمی شود.

۴- به فرزندانتان تأکید کنید که هرگز آدرستان، شماره تلفن یا سایر اطلاعات شخصی شامل جایی که به مدرسه می روند یا جایی که دوست دارند بازی کنند را ارسال نکنند.

۵- به کودکان بیاموزید که تفاوت بین درست و غلط در اینترنت همانی است که در دنیای واقعی وجود دارد.

۶- به کودکان بیاموزید که چگونه به دیگر استفاده کنندگان از اینترنت، احترام بگذارند. مطمئن شوید که آنها می دانند قواعد رفتار خوب فقط به دلیل اینکه پشت کامپیوتر هستند، تغییر نمی کند.

۷- به فرزندان تأکید کنید که به دارایی های دیگر کاربران احترام بگذارند. برایشان توضیح دهید که کپی های غیرقانونی از کارهای دیگران – مانند موسیقی، بازیهای تصویری و سایر برنامه ها- مانند دزدیدن آنان از یک فروشگاه است.

۸- به کودکان بگویید که هرگز نباید دوستان اینترنتی خود را شخصاً ملاقات کنند. توضیح دهید که دوستان اینترنتی ممکن است همانی که خود می گویند، نباشند.

۹- به کودکانتان بیاموزید که هرچه که می خوانند و می بینند، صحیح نیست. آنها را تشویق کنید که در مورد صحت مطالب اینترنت از شما سؤال کنند.

۱۰- فعالیت های اینترنتی کودکان خود را با نرم افزارهای پیشرفته کنترل کنید. کنترل های اینچنینی می توانند به شما در تصفیه کردن محتویات مضر، آگاهی از سایت هایی که کودکانتان سر می زنند و فهمیدن آنچه انجام می دهند، کمک کنند.

مراقب سوء استفاده از وب کم خود باشید

به راستی چقدر از امنیت اطلاعات شخصی خود در فضای مجازی مطمئن هستید. همه کاربران اینترنت و به خصوص افراد تازه کار از چند جبهه تحت هجوم قرار دارند. از یک سو دولت ها و سازمان های جاسوسی آنها، سعی در سرقت اطلاعات شهروندان دارند. از سوی دیگر هکرها و خرابکاران مستقل مدام در حال نفوذ به حریم خصوصی افراد هستند. و در نهایت این شرکت های بزرگ چند ملیتی هستند که با ادعای تبلیغات هدفمند، به فروش و بعضاً سوء استفاده از اطلاعات کاربران می پردازند.

احتمالاً اصطلاح «آزار جنسی سایبری» به گوشتان خورده است. مدتی است که محققان به ویژه جامعه شناسان و روان شناسان حوزه امنیت روانی خانواده از بابت وجود و بسط این پدیده در فضای مجازی اخطار می دهند. نا آگاهی افراد از مخاطرات پیش رو در فضای مجازی راه نفوذ و سوء استفاده افراد سودجو را هموارتر می کند.

طی بررسی های به عمل آمده و همچنین طبق گزارشی از سوی «یورو نیوز» وب کم ها یکی از موارد به شدت آسیب‌پذیر کاربران اینترنت هستند که روزانه هزاران قربانی می گیرند. در این بررسی مشخص شده که تعداد کسانی که به نفوذ و ضبط تصاویر وب کم کاربران در فضای مجازی می پردازند، به علت سهولت انجام این کار بسیار زیاد است و این در حالی است که اکثر قربانیان از دانش کافی برای جلوگیری از آن برخوردار نبوده اند.

آن‌ها با ضبط ویدیوی قربانیان خود یا آن ویدیوها را به اشخاص دیگر می فروشند، یا برای منتشر نکردن تصاویر از قربانی باج طلب می‌کنند. یا حتی او را مجبور به نشان دادن دیگر اعضای بدن خود می کنند. اینها و دیگر موارد از این دست مادامی که خود کاربران در صدد حفظ حریم خود بر نیایند تمامی نخواهد داشت.

به یاد داشته باشید که نگهبان اصلی و نهایی اسرار شما، خودتان هستید و هرگز نباید از کنار این مسأله بی تفاوت بگذرید. برای پیشگیری و ممانعت از نفوذ خرابکاران به وب کم رایانه راه کارهایی وجود دارد که البته همه آن‌ها فقط در صورتی که با هم به کار برده شوند مؤثر خواهند بود:

ضد بدافزارها و فایروال ها فقط زمانی مفید هستند که به هنگام باشند. روزانه هزاران ویروس و تروجان ساخته می‌شود که می‌توانند راه نفوذ به وب کم و رایانه شما را برای خرابکاران هموار کنند، و فقط زمانی می‌توانید جلوی آنها را با آنتی ویروس ها بگیرید که به روز باشند .

-مراقب ایمیل از سوی افراد ناشناس باشید. بهتر است به طور کل ایمیل‌های ناشناس را باز نکنید. ولی در صورت باز کردن، هرگز روی لینک های احتمالی موجود در آن کلیک نکنید .

-از اعتبار سایت هایی که برای ثبت نام، ایمیل شما را می خواهند مطمئن شوید. بسیاری از سایت ها و حتی تالارهای گفتگو با مبالغ ناچیز حاضر به فروش ایمیل های کاربران خود به اشخاص ثالث می شوند .

-وقتی از وب کم خود استفاده نمی‌کنید اگر قابلیت بستن لنز در آن وجود دارد آن را ببندید در غیر این صورت یا روی آن را بپوشانید یا آن را به سمت دیوار بگردانید .

-اگر حین گپ با غریبه ای احساس نزدیکی بیش از حد کردید، قبل از تبادل تصویر به خود متذکر شوید که او می‌تواند این مکالمه تصویری را ضبط و احیاناً منتشر کند .

-قبل از هرکاری راه و رسم آن را باید آموزش داد. والدین باید بدانند همان‌طور که فرزند خود را به کلاس شنا و زبان و... می‌فرستند تا آموزش‌های لازم را ببیند، نباید او را بدون آموزش در دریای متلاطم و بی رحم اینترنت و شبکه‌های مجازی رها کنند .

-با مهربانی باید کودکان را ترغیب کرد که اگر از طریق وب کم مورد سوءاستفاده قرار گرفتند به والدین خود گزارش دهند تا از گسترش قضیه جلوگیری شود .

-خود شما هم اگر حس کردید که ممکن است قربانی شده باشید به مراجع ذیصلاح اطلاع دهید .

-در همه حال مراقب باشید و چشم از چراغ وب کم خود بر ندارید!

شکارچیان آنلاین

یکی از مهمترین ویژگی‌های اینترنت گمنامی است. بسیاری از سودجویان از جمله شکارچیان آنلاین از همین ویژگی برای رسیدن به اهداف شوم خود استفاده می‌نمایند. بیشترین هدف شکارچیان آنلاین کودکان و نوجوانانی هستند که از لحاظ عاطفی مشکلات عمده‌ای را در خانواده خود دارند. در واقع این دسته از شکارچیان با ابزار همدردی با کودکان طرح دوستی با آنها می‌ریزند در حالی‌که این دوستی یک دوستی کاذب می‌باشد.

شکارچیان آنلاین به راحتی با مشاهده پروفایل کودکان و نوجوانان در شبکه‌های اجتماعی و چت روم ها و بررسی اطلاعات آنها نظیر مشخصات مدرسه، باشگاه ورزشی و حتی یک عکس ساده که یک شخص با ماشین شخصی و یا خانوادگی خود در جلوی منزلش گرفته و برای دوستان به اشتراک گذاشته اهداف خود را مشخص می نمایند. معمولا شکارچیان آنلاین از روش های متفاوتی جهت جلب اعتماد و مخفی نگه داشتن ارتباط فرزندان از والدین خود استفاده می کنند که مهمترین آنها عبارتند از: ارسال شارژ رایگان برای تلفن‌های همراه که این عمل به منظور مخفی نگه داشتن هزینه تلفن از والدین صورت می‌گیرد. از جمله موارد دیگری که جهت جذب استفاده می شود، ارسال عکس‌های شهوت انگیز برای نوجوانان است که متأسفانه بسیاری از قربانیان به این روش مورد حمله قرار گرفته اند.

نشانه های مهم در معرض خطر قرار گرفتن کودکان:

گرچه زیر نظر داشتن کودکان به طور کامل امری دشوار به نظر می‌رسد اما والدین با رعایت چند نکته که در زیر اشاره خواهد شد می‌توانند رفتار فرزندان خود را به منظور محافظت آنها در برابر شکارچیان اینترنتی کنترل نمایند.

نشانه های خطر:

۱) فرزندان زمان زیادی را به صورت آنلاین سپری می‌کنند.

۲) یافتن تصاویر و فیلم‌های غیرمجاز بر روی سیستم کامپیوتر فرزندان.

۳) دریافت تماس‌های تلفنی، ای‌میل و هدیه از طرف کسانی که شما آنها را نمی شناسید.

۴) خارج شدن فعالیت فرزندان از حالت طبیعی.

۵) سوییچ کردن صفحه در حال مشاهده کودکان زمانی که شما بر روی سیستم حضور پیدا می‌کنید.

۶) استفاده از حساب های کاربری متعدد (ای‌میل های جانبی) توسط فرزندان شما.

رایج ترین ابزارهایی که توسط شکارچیان آنلاین جهت اغفال کودکان بر روی اینترنت استفاده می‌شوند شامل اتاق های گفتگو، پیام‌های فوری و ایمیل می‌باشند. در واقع ۸۹ درصد سوءاستفاده جنسی آنلاین از طریق اتاق های چت و یا پیام از طریق مسنجر صورت یافته است.

پایان

منابع :

پلیس فتا (http://www.cyberpolice.ir)

اینترنت

با احترام

رضا فریدون نژاد

rezaf1390@gmail.com

مجموعه کتابهای الکترونیکی

دانش و زندگی

کتابهایی مختصر ، مفید و کاربردی

دانلود کاملاً رایگان

WWW.DZBOOK.IR

گردآوری و تنظیم : رضا فریدون نژاد