



ایجاد فضای امن مجازی برای کودکان

پیش زمینه

امروزه زندگی بچه های ما بیش از هر زمان دیگری به صورت آنلاین است، از معاشرت با دوستان و بازی گرفته تا یادگیری و آموزش آنلاین. بنابراین ما چگونه می توانیم به فرزندانمان کمک کنیم تا با خیال راحت و ایمن از فناوری آنلاین، بهترین استفاده را ببرند؟

آموزش و ارتباطات

اولین و مهمترین نکته این است که ارتباط خوب و محکمی با فرزندان خود برقرار کنید. بیشتر مواقع، والدین درگیر فناوری های مورد نیاز برای مسدود کردن محتوا یا تشخیص خوب یا بد بودن برنامه های تلفن همراه می شوند. در نهایت، ایمن نگه داشتن کودکان کمتر به فناوری مربوط بوده و بیشتر به رفتار و ارزش ها ربط دارد. باید شروع کنیم به نوشتن فهرستی از انتظاراتی که از فرزندانمان داریم. بعضی از موارد پیشنهادی که میتواند در نظر بگیرید به شرح زیر است (این موارد را میتوان با رشد و بزرگتر شدن بچه ها تغییر داد):

- در مورد زمان هایی که می توانند یا اجازه ندارند برای سرگرمی آنلاین شوند و برای مدت زمان آن تصمیم بگیرید. برای مثال، ممکن است بخواهید مطمئن شوید که بچه ها قبل از بازی آنلاین یا حضور در شبکه های اجتماعی با دوستانشان، تمام تکالیف یا کارهای خانه را انجام می دهند و مدت زمانی را که هر روز به صورت آنلاین می گذرانند محدود کنید.
- انواع وبسایتها، برنامه های تلفن همراه و بازی هایی را که می توانند به صورت آنلاین به آنها دسترسی داشته باشند و دلیل اینکه مناسب هستند یا نه را شناسایی کنید.
- مشخص کنید که آنها چه اطلاعاتی را و با چه کسانی میتوانند به اشتراک بگذارند. بچه ها اغلب متوجه نمی شوند که مطالبی که به صورت آنلاین ارسال می کنند عمومی، دائمی و برای هر کسی در دسترس خواهد بود. علاوه بر این، هر چیزی که به صورت خصوصی با دوستان خود به اشتراک می گذارند، می توانند (و اغلب همینطور است) با دیگران به اشتراک بگذارند بدون اینکه آنها اطلاع داشته باشند.
- مشخص کنید که آنها باید مشکلات را به چه کسانی گزارش دهند، مانند پنجره های بازشو عجیب، وب سایت های ترسناک، یا اینکه فردی که آنلاین است یک قلدر یا فردی عجیب و غریب است. بسیار مهم است که کودکان از صحبت کردن با یک بزرگسال مورد اعتماد احساس امنیت کنند.
- درست مانند دنیای واقعی، به کودکان بیاموزید که به صورت آنلاین با دیگران همانطور رفتار کنند که دوست دارند با آنها با احترام و وقار رفتار شود.
- اطمینان حاصل کنید که کودکان درک می کنند که افراد آنلاین ممکن است آن چیزی نباشند که ادعا می کنند و همه اطلاعات دقیق یا واقعی نیستند.
- تعریف کنید چه چیزی را می توان به صورت آنلاین و توسط چه کسی خریداری کرد، از جمله خریدهای درون بازی.

با گذشت زمان، هرچه رفتار بهتری داشته باشند و اعتماد بیشتری کسب کنند، ممکن است بخواهید با آنها با انعطاف بیشتری رفتار کنید. دستورات و انتظارات را که کامل فهرست کردید، میتوانید آنها را به دیوار نصب کنید. حتی بهتر از آن، از فرزندانمان بخواهید در قوانین مشارکت کنند و سند را امضا کنند تا همه با هم موافقت داشته باشند.

هر چه زودتر شروع به صحبت با کودکان کنید، بهتر است. اگر نمیدانید چگونه سر صحبت را باز کنید، موارد زیر پیشنهاد میشود. از آنها بپرسید که از کدام برنامه ها استفاده می کنند و چگونه کار می کنند. از آنها بخواهید مثل یک معلم به شما نشان بدهند که چه کارهایی روی اینترنت انجام میدهند. در نظر بگیرید که برای تقویت رفتارهای دیجیتال مثبتی که درباره آنها صحبت کرده اید یا با آنها موافقت کرده اید، سناریوهای "چه می شود اگر..." به آنها بدهید. سعی کنید این مکالمه دوستانه و مداوم باشد. این بهترین کار برای کمک به و محافظت از بچه ها در فضای مجازی است.

برای موبایل و تبلت ها سعی کنید که مکانی برای شارژ کردن باشد. قبل از اینکه فرزندان شما شب ها به رختخواب بروند، زمان مشخصی را در نظر بگیرید که همه دستگاه های تلفن همراه در ایستگاه شارژ قرار می گیرند تا کودکان شما وسوسه نشوند که از آنها در زمانی که باید بخوابند استفاده کنند.

فن آورهایی امن سازی و کنترلی برای والدین

فناوری های امنیتی و کنترل های والدینی وجود دارد که می توانید از آنها برای نظارت و اجرای قوانینی که تعیین کرده اید استفاده کنید. این راه حل ها بیشتر برای کودکان کم سال کار میکنند. بچه های بزرگ تر نه تنها به دسترسی بیشتری به اینترنت نیاز دارند، بلکه اغلب از دستگاه هایی استفاده می کنند که ممکن است کنترل آنها را نداشته باشید یا نتوانید آنها را کنترل کنید، مانند دستگاه های مدرسه، کنسول های بازی، یا دستگاه هایی در خانه دوستان یا خویشاوندان. علاوه بر این، کودکان بزرگتر اغلب می توانند تلاش های صرفاً تکنولوژیکی را برای کنترل خودشان دور بزنند. به همین دلیل است که در نهایت، ارتباط، ارزش ها و اعتماد با کودکان بسیار مهم است.

برای فرزندان الگو باشید

به یاد داشته باشید که به عنوان والدین یا سرپرست الگوی خوبی باشید. وقتی فرزندان با شما صحبت می کنند، دستگاه دیجیتال خود را زمین بگذارید و تمام توجه خود را به آنها معطوف کنید. در نظر داشته باشید که از دستگاه های دیجیتالی سر میز شام استفاده نکنید و در حین رانندگی پیامک ارسال نکنید. در نهایت، وقتی بچه ها اشتباه می کنند، به جای تنبیه، با هر یک از اشتباهات به عنوان تجربه ای برای یادگیری رفتار کنید. اطمینان حاصل کنید که وقتی هر چیزی ناراحت کننده را تجربه می کنند یا متوجه می شوند که اشتباهی آنلاین انجام داده اند، از نزدیک شدن به شما احساس امنیت می کنند.



سرديپر مهمان

دایانا کلی یکی از اعضای هیئت مدیره در WiCyS و CISO در Protect AI است. او مدرس دوره آموزشی لینکدین است: خطرات امنیتی در هوش مصنوعی (هوش مصنوعی) و ML (یادگیری ماشین) و نویسنده همکار کتاب معماری عملی امنیت سایبری.

منابع

بازی کردن آنلاین ایمن: <https://www.sans.org/newsletters/ouch/securely-gaming-online>
حریم خصوصی: محافظت از ردیای دیجیتال <https://www.sans.org/newsletters/ouch/privacy>
استفاده ایمن از دستگاه های تلفن همراه: <https://www.sans.org/newsletters/ouch/securing-mobile-devices>
دیب فیک: <https://www.sans.org/newsletters/ouch/learn-a-new-survival-skill-spotting-deepfakes>

ترجمه شده برای عموم توسط: هومن خجاو، مجید هدایتی

IOUCH توسط SANS Security Awareness منتشر شده است و تحت مجوز Creative Commons BY-NC-ND 4.0 می باشد. شما آزاد هستید که این ماهنامه را برای بقیه اشتراک گذاشته یا آن را توزیع نمایید به شرطی که آن را به فروش نرسانده یا تغییری در آن ایجاد نکنید. هیئت تحریریه: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.