معاونت آموزش ابتدایی
دفتر آموزش دبستانی
گروه برنامه ریزی، فناوری و گروه های آموزشی

رایا آموز

آموزش مهارت های برنامه نویسی و سواد دیجیتال
ویژه معلمان و دانش آموزان دوره ابتدایی

محور پنجم

سواد دیجیتال

شهروندی دیجیتال

شناسایی و توصیف اقدامات بالقوه ناامن و مضر در فضاهای آنلاین

نمونه محتوای آموزشی ویژه دانش آموزان

تهیه شده در گروه های آموزش ابتدایی دفتر آموزش دبستانی

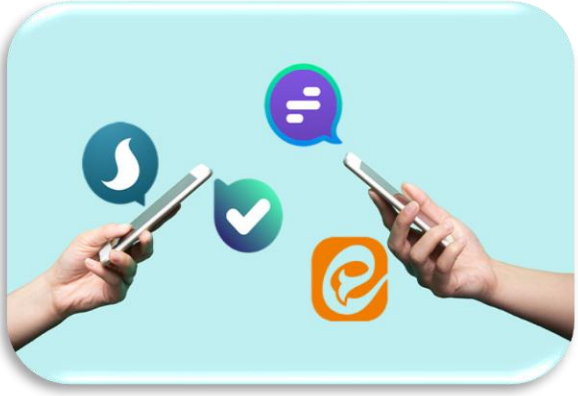
گردآورنده:فرید بهردار

تیم پشتیبان: مهندس احمد اسمعیلی ، میترا مرتضوی
دکترشبنم وداد تقوی، فاطمه قاسمی، معصومه اسداله زاده، مهدیه نیکویی

پایه ششم

آیا می دانید؟

اگر در فضای مجازی شخصی شما را تهدید کند، چه کاری می توانید انجام دهید؟



اگر از فرد ناشناسی لینکی به دست شما برسد، چه می کنید؟

خوب است بدانیم

با استفاده از اینترنت می‌توان با هرکسی در هر کجای این کره خاکی ارتباط برقرار کرد، با چند کلیک ساده یا لمس صفحه‌نمایش می‌توان از علوم و فنون مختلف مطلع شد، کارها و پروژه‌های مختلف را به‌صورت دورکاری انجام داد، معاملات مالی و بانکی را بی‌دغدغه و به‌سادگی هرچه تمام‌تر انجام داد. با این حال، فضای اینترنت ضرر و زیان‌هایی نیز دارد که در ادامه، با برخی از آسیب‌های فضای مجازی برای کودکان آشنا خواهیم شد.

۱_ آسیب به سلامتی و تندرستی:

کم‌تحرکی، اختلال‌های حرکتی، خستگی چشم، چاقی و اضافه‌وزن ازجمله آسیب‌هایی هستند که سلامت جسمانی کودکانی را که زیاد با دستگاه‌های دیجیتالی و فضای مجازی سر و کار دارند را تهدید می‌کنند.

۲_ سوءاستفاده از کودکان و زورگویی اینترنتی

احتمال اینکه کودکان و نوجوانان در فضای مجازی در معرض سوءاستفاده و زورگویی اینترنتی قرار بگیرند، از هر گروه سنی دیگری بیشتر است و کودکان از این جهت بسیار آسیب‌پذیرند.

افرادی هستند که با اهداف پلیدی وارد فضای مجازی می‌شوند و با هدف زورگویی اینترنتی برای محقق‌کردن این اهداف به‌دنبال طعمه می‌گردند. این افراد با درست‌کردن پروفایل‌های جعلی با کودکان دوست می‌شوند و پس از گذشت مدتی آن‌ها را در معرض تهدیدهای مختلفی مثل دریافت اطلاعات شخصی قرار می‌دهند و با برقراری ارتباط با کودکان به آنها آسیب رسانده و برای آنها خطر ایجاد می کنند.

عده دیگری هم هستند که پس از جلب‌اعتماد کودک، اطلاعات شخصی نظیر حساب‌های بانکی والدین درخواست می‌کنند و به این صورت کلاهبرداری هایی انجام می دهند.

۳_نصب نرم افزارهای مخرب از طریق اینترنت

گاهی اوقات هنگام جستجو در وب با وب سایت هایی روبه رو می شوید که با کلیک روی محتوای آن برنامه های مخرب یا ویروس ها بر رایانه نصب شده و از این طریق اقدام به سرقت اطلاعات یا هک سیستم می کنند.

عزیزان اگر مورد هدف زورگویی قرار گرفتید، همیشه می‌توانید روی کمک اولیا حساب کنید (چه زورگویی اینترنتی باشد و چه رودررو). همچنین می توانید از پلیس فتا کمک بگیرید.

راهکارهای مناسب برای محافظت در برابر این آسیب‌ها

۱. استفاده از نرم‌افزارهای امنیتی و محافظ

نرم‌افزارهای مختلفی وجود دارند که با استفاده از آن‌ها می‌توانید دسترسی به وب‌سایت‌های نامناسب را محدود کنید. با برخی از نرم‌افزارها امکان نظارت بر فعالیت کودکان توسط والدین در فضای مجازی وجود خواهد داشت.

۲. آموزش استفاده به جا و مناسب از فضای مجازی

دانش آموز عزیز راهکارها و توصیه‌های زیر را مدنظر داشته باشید و عملی کنید:

- ❑ به‌اشتراک‌گذاری تصاویر شخصی و خانوادگی ممنوع است.
- ❑ رمزهای عبور خود را به‌هیچ‌عنوان نباید در اختیار دیگران بگذارید.
- ❑ قوانین خانوادگی استفاده از اینترنت داشته باشید و همه اعضای خانواده ملزم به رعایت آن‌ها باشند.

می توانید اطلاعاتی را که یاد گرفته اید با خانواده خود نیز مطرح کنید و سپس قوانینی طراحی کنید.

اگر در فضای مجازی صحبت با کسی شما را وحشت‌زده یا آزرده‌خاطر کرد، حتماً به اولیا اطلاع دهید.

- ❑ تحت هیچ شرایطی اطلاعات شخصی اعم از آدرس منزل، شماره تلفن، اسم یا آدرس مدرسه را در اینترنت فاش نکنید.
- ❑ تحت هیچ شرایطی نباید به ایمیل‌ها، پست‌ها، پیام‌ها و متن‌های تهدیدآمیز پاسخ دهید(اگر ارسال چنین پیام‌هایی مکرر و آزاردهنده شد، مسئله را با والدین و پلیس فتا در میان بگذارید).

چگونه بررسی کنیم که وب‌سایتی بدافزار دارد یا نه؟

۱- وب سایت های انتقال پول بانک ها از https به جای http استفاده می کنند.

هنگامی که وارد سایتی می‌شوید به آدرس آن دقت کنید، اگر با https:// شروع شود به این معنی است که اطلاعات فرستاده شده بین مرورگر شما و سرور این وب‌سایت به صورت رمز شده انتقال می‌یابند. اگر با http:// شروع شود یعنی باید مراقب فرستادن اطلاعاتی مانند نام کاربری و رمزعبور، خرید آنلاین و غیره باشید، زیرا اطلاعات رمز نشده انتقال می‌یابند. هنگام اتصال به درگاه های پرداخت به https توجه کنید.

۲- توصیه هایی برای خریدهای اینترنتی یادآوری می شود.

اگر در هنگام خریدهای اینترنتی، آگاهی لازم را نداشته باشید، ممکن است اطلاعات بانکی شما توسط هکرها به سرقت رفته و حساب بانکی شما یا والدین خالی شود. برای جلوگیری از این اتفاق موارد زیر را رعایت کنید:

- بدون اجازه بزرگ تر ها اقدام به خریدهای اینترنتی نکنید.
- فریب تبلیغات و تخفیفات و یژه را نخورید.
- از سایت های معتبر خرید کنید .
- سایت دارای enamadباشد.
- به علامت شاپرک در درگاه ورودی اطلاعات بانکی توجه کنید.
- از صفحه کلید مجازی خود رایانه برای وارد کردن اعداد استفاده نمایید.

۴- تمام نرم‌افزارهایتان را به روز نگاه دارید.

- به روز نگاه داشتن تمام نرم‌افزارهایتان که هیچ زحمتی هم برایتان ندارد یکی ازبزرگ ترین راه‌های آلوده نشدن به بدافزارهاست. همواره آخرین نسخه نرم افزارها، به خصوص مرورگرها و آنتی ویروس ها را نصب نمائید.

امروزه به اشتراک گذاری اطلاعات در فضای مجازی امری عادی شده است. هر محتوایی که ارسال می کنید باید به عواقب، نتایج و بازخوردهای آن نیز توجه کنید.

امروزه اکثر وب سایت ها یک نسخه بایگانی از محتوای خود را نگه می دارند. این مورد از بسیاری جهات مانند دسترسی به فایل ها و مطالب قدیمی بسیار خوب است. اما این مورد معایبی نیز دارد. فرض کنید شما اشتباهاً عکسی را در فضای مجازی به اشتراک گذاشته اید، هنگامی که متوجه اشتباه خود می شوید و عکس را پاک می کنید، ماجرا تمام نمی شود، یک بایگانی از تصاویر در اینترنت وجود دارد و ممکن است با یک جستجوی ساده، حتی پس از حذف عکس، امکان دسترسی به آن باشد.

پس سعی کنید اطلاعات شخصی مانند: تصاویر، نشانی، شماره تماس را تا آنجا که ممکن است در اینترنت و وب سایت های مختلف قرار ندهید.

آنچه آموختم

دانش آموز عزیز

جهت استفاده صحیح و مناسب از فضای مجازی به چه نکاتی باید توجه کرد؟

در کنار خانواده خود یک وب سایت را بررسی کنید که اطلاعات مفیدی دارد یا مخرب است؟