➢ نکات مهم در امنیت خرید اینترنتی

با افزایش روز به روز تعداد کاربران اینترنت، اکثر مردم برای انجام امور گوناگون، از امور آموزشی و تفریح و سرگرمی گرفته تا امور اداری و تجاری از این شبکه جهانی کمک گرفته و همه چیز رنگ و بوی اینترنتی گرفته است. حتی گروه زیادی برای رفع نیازهای روزمره خود و خریدهای روزانه و...از طریق خرید اینترنتی اقدام کرده و در این صورت در وقت و هزینه نیز صرفه‌جویی می‌کنند.

یکی از مشکلاتی که در همین چند سال، از به وجود آمدن پدیده‌ی خرید اینترنتی وجود دارد عدم اطلاع کاربران از نکات ریزی است که سبب می‌شود خرید آنلاین به منبعی برای سودجویان جهت اخاذی از کاربران تبدیل شود. پیش از آن که کالای جدیدی را به سبد خرید خود اضافه کنید باید از به روز بودن و در اختیار داشتن آخرین نسخه نرم افزار امنیتی، مرورگر وب و سیستم عامل دستگاه خود اطمینان حاصل کنید. پاکسازی دستگاه بهترین اقدام دفاعی در برابر ویروس ها، بدافزارها و دیگر تهدیدهای آنلاین محسوب می شود .

زمانی که قصد خرید اینترنتی و پرداخت اینترنتی یا واریز وجه به فروشگاهی را دارید باید از معتبر بودن آن سایت اطمینان داشته باشید.برای انجام خرید اینترنتی امن نکاتی مهمی را که در ادامه می خوانید به شما کمک شایانی خواهد کرد.

چند نکته برای انجام خرید آنلاین امن را ارائه می کنیم:

- کنترل فروشندگان

پیش از خرید آنلاین اندکی زمان صرف کرده و درباره فروشنده ای که تاکنون با وی معامله نداشته اید، پژوهش کنید. برخی از افراد سودجو و مهاجمان تلاش می کنند با ایجاد وب سایت های مخرب و آلوده که به نظر قانونی می رسند، خریداران را فریب دهند.

- حصول اطمینان از قانونی بودن وب سایت فروشنده

پیش از آن که اطلاعات شخصی و مالی خود را برای انجام تراکنش آنلاین وارد کنید، نشانه های امن بودن وب سایت را مورد بررسی قرار دهید. این بررسی شامل مشاهده یک نماد قفل در نوار آدرس و یا آدرسی است که با shttp یا https آغاز می شود .

- حفاظت از اطلاعات شخصی

هنگامی که خرید آنلاین انجام می دهید نسب به اطلاعاتی که برای تکمیل تراکنش جمع آوری می شوند، هوشیار باشید. اطمینان حاصل کنید که ارائه این اطلاعات به فروشنده ضروری است. این نکته را فراموش نکنید که شما تنها باید بخش های ستاره دار و ضروری فهرست خرید فروشنده آنلاین را پر کنید.

- استفاده از گزینه های پرداخت امن

به طور کلی، کارت های اعتباری امن ترین گزینه برای پرداخت آنلاین هستند زیرا خریدار در صورت عدم دریافت محصولی که سفارش داده و یا دریافت محصولی دیگر می تواند شرایط ایجاد شده را پیگیری کند. همچنین، اگر کارت اعتباری به سرقت رفته و یا توسط فرد دیگری استفاده شود می توانید میزان پول برداشتی از آن حساب را محدود و یا مسدود کنید.

- حفظ اطلاعات خرید

تراکنش های آنلاین خود شامل توضیح محصول، قیمت، رسید آنلاین، شرایط فروش و کپی های هر ایمیلی که با فروشنده را چاپ و نگهداری کنید .

- خاموش کردن رایانه پس از اتمام خرید

بسیاری از مردم رایانه خود را در طول شبانه روز روشن و همواره متصل به اینترنت نگه می دارند. این به کلاهبرداران اجازه می دهد تا به دستگاه کاربر دسترسی داشته و با نصب بدافزارها اقدام به جرایم سایبری کنند. برای حفظ امنیت پس از اتمام استفاده، رایانه خود را خاموش کنید.

- احتیاط نسبت به ایمیل های درخواست اطلاعات

مهاجمان سایبری ممکن است از طریق ارسال ایمیل درخواست تایید خرید، اطلاعات حساب کاربری و یا بانکی خریدار را داشته باشند. به این نکته توجه کنید که کسب و کارهای قانونی هرگز چنین اطلاعاتی را از طریق ایمیل دریافت نمی کنند.

- حساب کاربری منحصر به فرد، گذرواژه منحصر به فرد

از یک گذرواژه برای حساب های کاربری مختلف خود استفاده نکنید زیرا به مجرمان سایبری کمک می کند تا هرچه راحت تر به اطلاعات شخصی شما دست یابند.

- انتخاب گذرواژه های طولانی و قوی

در گذرواژه های خود از حروف بزرگ و کوچک به همراه اعداد و نمادها حداقل به میزان هشت کاراکتر استفاده کنید تا از ترکیبی قدرتمند برخوردار شوید.

➢ دسترسی کنترل‌نشده به اینترنت، تهدیدی برای کودکان

برخورد کودک با محیط مجازی و مراقبت های لازم آن:

بیشتر والدین نمی‌دانند که نظارت، کنترل و راهنمایی شان را باید هنگام استفاده از اینترنت اعمال کنند و نگذارند کودکشان به راحتی و بدون هیچ نظارتی به محیط مجازی وراد شود.

در نظر گرفتن ایمنی کودکان در فضای مجازی از اهمیت ویژه‌ای برخوردار بوده و از این طریق والدین می توانند در بهترین موقعیت ممکن هدایت دقیق و مسئولانه فرزندان خود در فضای مجازی را بر عهده بگیرند.

در نظر گرفتن ایمنی کودکان در فضای مجازی از اهمیت ویژه‌ای برخوردار بوده و از این طریق والدین می توانند در بهترین موقعیت ممکن هدایت دقیق و مسئولانه فرزندان خود در فضای مجازی را بر عهده بگیرند.

از این رو، آگاهی و شناخت از خطرات موجود در این زمینه و برنامه ریزی مناسب پیش از فراهم کردن دسترسی به اینترنت برای کودکان از اهمیت ویژه‌ای در دنیای امروز که شاهد آهنگ سریع پیشرفت فناوری است، برخوردار می شود. در ادامه این مطلب گزیده‌ای از خطرات و همچنین اقدام‌های لازم برای حضور ایمن کودکان در فضای مجازی را بیان می کنیم.

- **خطرات**

- در فضای مجازی، امکان برقراری تماس‌های نامناسب کودکان با افرادی که ممکن است قصد سوء استفاده، بهره برداری و یا تجاوز به حریم خصوصی آنها را داشته باشند، وجود دارد.

- در فضای مجازی، امکان بروز رفتارهای نامناسب کودکان به واسطه تاثیرپذیری از شیوه‌های برخورد آنلاین دیگران مانند ارائه اطلاعات شخصی در مکان‌هایی که افراد بسیار زیادی به آنها دسترسی خواهند داشت، وجود دارد. بر همین اساس، امکان تبدیل شدن کودکان و نوجوانان به عامل و یا هدف "زورگیری سایبری*" وجود دارد.

- در فضای مجازی، امکان دسترسی به محتوای نامناسب مانند فیلم‌ها، تصاویر، مطالب و نوشته‌های غیر اخلاقی، نژادپرستانه، خشونت آمیز و دیگر موارد مضر و خطرناک یکی دیگر از مواردی است که کودکان و نوجوانان را به شدت در معرض تهدید قرار می دهد.

ایمن نگه داشتن کودکان در فضای آنلاین

روش‌های مختلفی برای ایمن نگه داشتن کودکان هنگام حضور آنها در فضای مجازی وجود دارد. بی تردید، یکی از موثرترین روش‌ها در این زمینه آموزش آنها از سنین پایین و آشنایی و افزایش آگاهی کودکان درباره خطراتی است که امکان مواجه شدن با آنها در فضای مجازی وجود دارد.

همچنین، کودکان باید چگونگی شناسایی این تهدیدها و خطرات و اقدام‌های ضروری برای مقابله با آنها را فرا بگیرند. منابع آموزشی مناسبی برای والدین، معلمان و حتی خود کودکان وجود دارند که ابعاد مختلف ایمنی کودکان در فضای آنلاین را پوشش می دهند.

کودکان هرگز نباید بدون نظارت فردی بالغ با فرد یا افرادی که در دنیای مجازی ارتباط داشته‌اند، در دنیای واقعی نیز ملاقات داشته باشند.
ارتباط نزدیکی با کودکتان برقرار کرده و با افزایش حس اطمینان در وی، این امکان را فراهم کنید تا درباره نگرانی‌های خود پیرامون مکالمات، پیام‌ها و یا رفتارهایی که در فضای مجازی داشته است، صحبت کند.
کودکان را تشویق کنید تا تجربه حضور خود در اینترنت را با شما به اشتراک گذاشته و آن را به یک تجربه خانوادگی مبدل کنند.
از کودکان بخواهید تا هر گونه زورگویی‌های سایبری را به سرعت و از طریق گفت و گوی حضوری و یا تلفنی به شما اطلاع دهند.