OUCH! ژوئیه 2022

ماهنامه آگاهی از امنیت اطلاعات برای شما

بازی آنلاین به صورت ایمن

موردی که بازی های آنلاین را جذاب و مفرح میکند این است که شما میتوانید از هر جای دنیا با دیگران بازی کرده و ارتباط برقرار کنید، حتی اگر اغلب کسانی که با آنها بازی میکنید را نشناسید. اگر چه اکثر قریب به اتفاق افراد آنلاین مانند شما برای تفریح و سرگرمی حضور دارند، اما اشخاصی نیز هستند که قصد آسیب رساندن را دارند.

خود را ایمن کنید

بزرگترین خطر بازی های آنلاین، تکنولوژی به کار رفته در آن نیست، بلکه تعاملی است که شما با افراد غریبه و ناشناس دارید.

- در مورد هر پیامی که از شما خواسته شده کاری را انجام دهید محتاط باشید، مانند کلیک کردن روی یک لینک یا دانلود کردن یک فایل. مهاجمان از پیامهای درون بازی یا ایمیلهای فیشینگ استفاده میکنند تا شما را فریب دهند و از شما بخواهند کاری را انجام دهید که ممکن است باعث آلوده شدن رایانه شما، دزدیده شدن هویت شما، یا اکانتهای بازی شما شود. اگر پیامی که در حین باری برای شما ارسال شده به نظرغیر عادی است، یا آنقدر خوب است که قابل باور نیست، مشکوک باشید چراکه ممکن است این مورد یک حمله باشد.
- بسیاری از بازیهای آنلاین فروشگاههای مالی خاص خود را دارند که میتوانید در آنجا داد و ستد کرده، معامله پایاپای انجام دهید، یا کالاهای مجازی خریداری نمائید. دقیقا مانند دنیای واقعی، در این فروشگاه ها نیزکلاهبردارهایی هستند که تلاش خواهند کرد که شما را فریب داده و پول شما یا هر نوع ارز مجازی را که دارید، بدزدند. تنها با اشخاصی ارتباط برقرار کنید که اعتبار و شهرت قابل اعتمادی کسب کرده اند.
- از عبارتهای عبور(رمز عبور با کلمات ترکیبی) قوی، منحصر به فرد برای هر یک از اکانتهای بازی استفاده کنید. با این روش مهاجمین نمیتوانند به سادگی رمزهای عبور شما را حدس زده و حسابهای شما را تصاحب کنند. اگر بازی/پلتفرم شما قابلیت احراز هویت دو مرحله ای را دارد، از آن استفاده کنید. نمی توانید همه رمزهای عبور خود را به خاطر بسپارید؟ ازبرنامه مدیریت رمزعبور استفاده کنید.

سیستم خود را ایمن کنید

مهاجمین ممکن است تلاش نمایند رایانه شما، یا دستگاهی که روی آن بازی میکنید را هک کرده و به آن تسلط یابند، شما میبایست برای حفاظت از آن اقدام کنید.

- دستگاههای خود را با استفاده از به روز ترین نسخه سیستم عامل و یا نرم افزارهای بازی و برنامه های بازی ایمن کنید.نرم افزارهای قدیمی و منسوخ شده دارای آسیب پذیریهای شناخته شده ای هستند که مهاجمان میتوانند از آنها بهره برداری کرده و با استفاده از آن دستگاه شما را هک کنند. به روز رسانی خودکار را در صورت امکان فعال نمائید. شما میتوانید با به روز نگه داشتن دستگاهها و برنامه های بازی خود، اکثر این آسیب پذیریهای شناخته شده را از بین ببرید.
- نرم افزارهای بازی و بسته های افزونه موجود بازی خود را تنها از وبسایتهای معتبر و شناخته شده دانلود نمائید. مهاجمان اغلب نسخه های جعلی یا آلوده ایجاد میکنند، سپس آن را از طریق سرور خود توزیع مینمایند. علاوه بر این، اگر هر بازی یا افزونه ای نیاز به غیر فعال کردن ابزار یا تنظیمات امنیتی توسط شما داشت، از آن استفاده نکنید.

- بازارهای زیرزمینی برای حمایت از فعالیتهای متقلبانه به وجود آمده اند. در کنار غیر اخلاقی بودنشان، بسیاری از برنامه های تقلب(Cheat)، خودشان بدافزار(Malware) هایی هستند که دستگاه شما را آلوده خواهند کرد. هرگز هیچ نوع نرم افزار یا وب سایت تقلبی را نصب و یا از آنها استفاده نکنید.
- هر نرم افزار بازی آنلاینی که استفاده میکنید، وب سایت آن را چک کنید .بسیاری از سایتهای بازی، بخشی در مورد چگونگی ایمن سازی شما و سیستم تان دارند.

برای والدین یا اولیا

آموزش و گفتگوی آزاد با بچه ها موثرترین قدمی است که میتوانید برای محافظت از فرزندانتان بدارید. یک رویکرد این است که از آنها بپرسید که به شما نشان دهند بازیهایشان چگونه کار میکنند،از آنها بخواهید به شما نشان دهند یک بازی معمولی چه شکلی است. چه بسا حتی میتوانید با آنها بازی کنید. علاوه بر این، از آنها بخواهید افراد متفاوتی را که به صورت آنلاین ملاقات میکنند برای شما توصیف کنند. اغلب اوقات بازی کردن آنلاین میتوانید بخش بزرگی از زندگی اجتماعی فرزند شما باشد. با صحبت کردن با آنها(وصحبت کردن آنها با شما) میتوانید یک مشکل را شناسایی کرده و بسیار موثرتر از هر فناوری دیگری از آنها محافظت نمائید. برخی از مراحل اضافی عبارتند از:

- بازی هایی که انجام میدهند را بشناسید و مطمئن شوید که طبق حس تان بازی ها برای سن کودک شما مناسب میباشد.
- مقدار اطلاعاتی را که کودکان شما به صورت آنلاین به اشتراک میگذارند، محدود کنید. به عنوان مثال، آنها هرگز نباید رمزهای عبور، سن، شماره تلفن یا آدرس منزل شان را به اشتراک بگذارند.
- در نظر داشته باشید میتوانید دستگاههای بازی آنها را در محیطی باز قرار داده تا بتوانید آنها را تحت نظر داشته باشید. علاوه بر این، بچه های کوچکتر نباید در اتاق خود و یا شبها تا دیروقت بازی کنند.
- قلدری، کلمات زشت، یا سایر رفتارهای ضد اجتماعی میتوانند مشکل ساز باشند. مراقب بچه های خود باشید، اگر بعد از انجام یک بازی ناراحت به نظر میرسند، ممکن است به صورت آنلاین تحت زورگویی و آزار و اذیت قرار گرفته باشند. اگر آنها به صورت آنلاین مورد آزار و اذیت قرار میگیرند، به سایت بازی گزارش داده و از فرزندان خود بخواهید فقط با دوستان قابل اعتماد خود بازی های آنلاین را انجام دهند.
- بیاموزید که آیا بازی های فرزند شما از خریدهای درون برنامه ای پشتیبانی میکنند و چه نوعی از ممانعت والدین(Parental overrides) را ارائه میدهد.

سردبیر مهمان

چارلی گلدنر موسس CyberNV و مربی SANS است. او در لینکدین فعال بوده و از سازمانهای دولتی پشتیبانی میکند. او در طول سالها، ساعتهای زیادی را روی رایانه های شخصی و کنسولها به بازی گذرانده است.

منابع

حملات مهندسی اجتماعی: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
احراز هویت چند مرحله ای: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers/
امنیت آنلاین برای کودکان: https://www.sans.org/newsletters/ouch/online-security-kids/

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو