وای! ژولای 2017

SafeNet Network & Security Services
شبکه امن اندیشه فردا

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- خودتان را امن کنید
- کامپیوترتان را امن کنید
- مخصوص والدین

بازی آنلاین امن و امان

مقدمه

یکی از بهترین راه های تفریح کردن بازی های آنلاین است و در عین حال این کار حاوی مجموعه ای از ریسک های منحصر بفرد خود نیز هست. در این خبرنامه روشهایی را بررسی میکنیم که چگونه شما و خانواده تان میتوانید در حین بازی آنلاین از خود محافظت کنید.

سردبیر مهمان

آقای استیو آرمسترانگ موسس Logically Secure ، مدرس موسسه SANS و معمار CyberCPR نرم افزار مدیریت حادثه میباشد. وی در توییتر با **@Nebulator** فعال است و با بسیاری از شرکتهای بزرگ تولید بازی همکاری میکند که از آرزوهای او در دوران کودکی بود.

خود را امن کنید

یکی از دلایلی که بازی آنلاین را لذت بخش میکند این است که شما میتوانید با دیگران در هر نقطه ای از دنیا بازی کرده و با آنها ارتباط برقرار کنید. تقریبا اکثر کسانی را که با آنها بازی میکنید نمیشناسید. درحالیکه اکثر کسانی که آنلاین هستند مثل شما هدفشان لذت بردن از بازی است افرادی نیز هستند که به دنبال آسیب رساندن هستند. در زیر گام هایی را عنوان میکنیم که لازم است شما برای امن کردن خود بردارید:

- نسبت به هرگونه پیغامی که از شما میخواهد اقداماتی مثل کلیک کردن بر روی یک لینک و یا دانلود کردن یک فایل را انجام دهید حساس باشید. مشابه حملات فیشینگ در ایمیل ها، هکرها در بازی های آنلاین نیز به دنبال این هستند تا با گول زدن شما از شما بخواهند عملی را انجام دهید که نتیجه آن آلوده شدن کامپیوتر شما و یا دزدیده شدن اطلاعات شما خواهد بود. اگر پیغامی عجیب و غریب با عنوان هایی مثل فوری یا ضروری و همچنین پیام هایی خیلی نزدیک به واقعیت که دور از انتظار است دریافت کردید، به آنها شک کنید چرا که ممکن است یک حمله باشند.
- بسیاری از بازی های آنلاین بازارهای مالی خاص خود را دارند که در آن بازارها شما قادر به معامله، تجارت و یا خرید اقلام مجازی خواهید بود. مشابه بازارهای واقعی، در محیط بازی مجازی نیز افراد فریبکاری هستند که تلاش میکنند تا با گول زدن شما پول و یا هرگونه سرمایه مجازی که جمع کرده بودید را بدزدند. تنها با افرادی که معامله کنید که خوشنام و قابل اعتماد هستند.
- برای حسابهای بازی های خود از کلمات عبور قوی استفاده کنید. به این ترتیب هکرها نمیتوانند به آسانی کلمه عبور شما را حدس بزنند و وارد حساب شما بشوند. اگر بازی امکانات رمز عبور دو عاملی را دارد، از آن استفاده کنید. برای هر بازی آنلاین یک حساب متفاوت داشته باشید. به این طریق اگر حساب یک بازی هک شد، بقیه حساب های شما امن خواهند بود. اگر نمیتوانید همه رمز های عبور خود را حفظ کنید، میتوانید از برنامه های مدیریت رمز عبور استفاده کنید.

کامپیوترتان را امن کنید

هکرها ممکن است تلاش کنند تا کامپیوتری که شما از آن برای بازی های آنلاین استفاده میکنید هک کنند. لازم است قدمهای ذیل را برای حفاظت از کامپیوتر خود بردارید.

بازی آنلاین امن و امان

کلید بازی کردن امن در محیط آنلاین استفاده از رمز عبور قوی، امن کردن کامپیوتر خود و کمی تفکر در صورت دریافت پیام ها و درخواست های مشکوک است.

- با اجرای آخرین نسخه از سیستم عامل و نرم افزار بازی کامپیوتر خود را امن کنید. برنامه های قدیمی و منسوخ حاوی آسیب پذیری هایی هستند که هکر ها میتوانند از آنها بهره برداری کرده و کامپیوتر شما را هک کنند. با به روز نگه داشتن کامپیوتر و برنامه های خود، بسیاری از این آسیب پذیری ها محدود خواهند شد.
- از آنتی ویروس استفاده کنید و مطمئن شوید که که آنها نیز به روز بوده و آلوده نبودن هر فایلی که اجرا میکنید را بررسی میکنند.
- نرم افزار های بازی را فقط از سایت های مطمئن دانلود کنید. بسیاری از مواقع هکرها با ایجاد نسخه تقلبی از نرم افزار های بازی و توزیع آن از طریق سرور ها خود به شما حمله میکنند.
- بسته های افزونه بازی ها که عموما به جهت افزودن ویژگی های جدید استفاده میشوند، غالبا در بخش انجمن(community) نوشته میشوند. گاهی اوقات هکرها این بسته ها را با بدافزار آلوده میکنند. همانطور که بازی را از سایت مطمئن دانلود میکنید، افزونه ها را نیز از سایت های قابل اطمینان دانلود کنید. در مجموع هر افزونه ای که از شما بخواهد آنتی ویروس خود را غیر فعال کنید و یا باعث ایجاد تغییرات در بخش امنیت شما شود، از آن استفاده نکنید.
- بازارهای زیرزمینی در حمایت از فعالیت های تقلبی مشغول بکار هستند. جدای از غیر اخلاق بودن این کار، بسیاری از برنامه های تقلبی حاوی بدافزار هستند که کامپیوتر شما را آلوده میسازند. هرگز برنامه های تقلبی را نصب نکنید و یا از سایت های تقلبی استفاده نکنید.
- بسیاری از سایت هایی که بازی های آنلاین ارائه میدهند شامل بخشی هستند که چگونه خود و کامپیوتر خود را امن کنید. حتما سایت شرکت نویسنده ی بازی را چک کنید.
- در خاتمه، همانطور که در زمان بازی آنلاین روی کامپیوتر خود مراقب هستید، روی موبایل خود هم مراقب باشید. هکرهای سایبری حمله به موبایل ها را نیز شروع کرده اند.

برای والدین

کودکان زمانی که از بازی های آنلاین استفاده میکنند نیازمند مراقبت و آموزش بسیار میباشند. آموزش و گفتگوی آزاد با کودکان یکی از موثرترین گام ها در جهت مراقبت از آنهاست. یکی از ترفندهای جالب برای تشویق کردن کودکان به صحبت کردن این است که از آنها درخواست کنید تا نحوه بازی کردن را به شما نشان بدهند، شما را وارد دنیای آنلاین بکنند و به شما نشان بدهند که یک بازی معمولی چگونه به نظر میرسد. شاید هم امکان باری کردن با آنها را داشتید. علاوه بر این از آنها بخواهید به شما در مورد افراد مختلفی که در محیط آنلاین ملاقات میکنند توضیح دهند. اکثر مواقع بازی های آنلاین میتوانند بخش اعظمی از زندگی اجتماعی کودکان شما باشند. باصحبت کردن با آنها (و اینکه از آنها بخواهید با شما صحبت کنند) میتوانید مشکل را شناسایی کرده و از آنها حتی بهتر از موثرترین تکنولوژی ها محافظت کنید.قدمهای بیشتر در ذیل توضیح داده میشود:

بازی آنلاین امن و امان

- بدانید که چه بازی هایی میکنند و مطمئن شوید آن بازی برای سن آنها مناسب است یا خیر.
- میزان اطلاعاتی را که کودکتان بصورت آنلاین به اشتراک میگذارد محدود کنید. بعنوان مثال، آنها نباید رمز عبور، سن، شماره تماس و یا آدرس منزل را به اشتراک بگذارند.
- با قراردادن کامپیوتر آنها در یک محیط باز آنها را تحت نظر بگیرید. علاوه بر این، کودکان جوانتر نباید در اتاق خود و یا تا دیروقت بازی کنند.
- زورگویی، بد زبانی و یا سایر رفتارهای ضداجتماعی میتواند یک مشکل باشد. چشم از کودک خود بر ندارید، اگر آنها بعد از بازی ناراحت به نظر میرسند ممکن است در فضای آنلاین به آنها زورگویی شده باشد. اگر مورد زورگویی آنلاین قرار گرفتند، از آنها بخواهید بازی را متوقف کرده و بازی را در محیط های کودکانه تر انجام دهند و یا از آنها بخواهید بازی های آنلاین را با دوستان مورد اعتماد ادامه دهند.
- یاد بگیرید که نرم افزار بازی کودکتان چه نوع کنترلی را برای والدین فراهم میکنند.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

شبکه خانگی خود را امن کنید:	https://securingthehuman.sans.org/ouch/2016#february2016
مهندسی اجتماعی:	https://securingthehuman.sans.org/ouch/2017#january2017
گذر عبارات:	https://securingthehuman.sans.org/ouch/2017#april2017
نرم افزارهای مدیریت رمز عبور:	https://securingthehuman.sans.org/ouch/2015#october2015
احراز هویت دو عاملی:	https://securingthehuman.sans.org/ouch/2015#september2015

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی