**شش محل که شما به سادگی در آنجا هک می شوید!!**

**کاربران اینترنت معمولاً برای یافتن عکس ها، ویدئوهای خنده دار، مقالات علمی و… خود در گوگل جستجو می کنند اما ممکن است در خلال همین جستجو ها به یکباره سیستم آنها با مشکلات جدی روبرو شود. بسیاری از متخصصان امنیتی، محیط مجازی را به میدان مین تشبیه کرده اند چراکه درست زمانیکه شما فکر می کنید همه جوانب امنیتی را رعایت کرده اید، به بدافزارهای کلاهبرداری آنلاین آلوده می شوید.**

**براساس این گزارش به بررسی موقعیت های خطرناک و همچنین محیط های ناامنی پرداخته که کاربران در مواجهه با این محیط ها و موقعیت ها باید هوشیاری بیشتری به خرج داده و بیشتر از قبل نکات امنیتی را رعایت کنند. در ادامه به بررسی هر یک از این موقعیت ها می پردازیم:**

**- موقعیت اول: فایل های مخرب فلش**

**محیط خطرآفرین: وب سایت های حاوی فایل های فلش**

**طی سال های اخیر نرم افزارهای گرافیکی ادوبی فلش به هدف مطلوب بدافزارها تبدیل شده اند. بطوریکه این شرکت بطور مداوم در حال انتشار اصلاحیه های امنیتی است. اما آنچه در این نرم افزار محل خطر است، کوکی های فلش است که به سازندگان آن این امکان را می دهد تا تنظیمات کمتری بر روی فلش اعمال کنند و از این طریق سایت هایی که شما بازدید کرده اید را ردیابی کنند. بدتر از آن زمانیست که حتی با حذف کوکی های مرورگر، باز هم کوکی های فلش در پشت صحنه باقی می مانند.**

**پس اگر شما از یک وب سایت حاوی فلش بازدید کردید، به منظور حفاظت در برابر حملات مبتنی بر فلش، پلاگین فلش مرورگر خود را بروز نگه داشته و قبل از هرگونه دانلود آن را با تنظیمات مرورگر خود بررسی کنید.**

**- موقعیت دوم: لینک های کوتاه شده**

**محیط خطرآفرین: توییتر**

**از زمان ایجاد توییتر، کلاهبردان اینترنتی سعی می کنند تا با استفاده از لینک های کوتاه شده کاربران را برای کلیک بر روی لینک های مخرب ترغیب کنند. چراکه پنهان کردن بدافزارها پشت لینک های کوتاه کار بسیار ساده تری است.**

**پس هر زمان که به سایت توییتر سر زدید به هیچ وجه بر روی هیچ لینکی کلیک نکنید. اگر هم می خواهید لینک های مخرب را از سالم تشخیص دهید از برنامه Tweet Deck که دارای ویژگی نمایش کامل لینک ها قبل از ورود به سایت است، استفاده کنید.**

**موقعیت سوم: ایمیل ها و فایل های پیوست**

**محیط خطرآفرین: Inbox ایمیل شما**

**اگرچه کلاهبرداری های فیشینگ و حملات مخرب به ایمیل ها اتفاق تازه ای نیست اما روش های این کلاهبرداری ها دائماً در حال تحول است. بطوریکه این روزها پیام های عادی از پیام های مخرب قابل تشخیص نیستند. به همین دلیل به کاربران توصیه می شود به هرآنچه که به Inbox شان وارد می شود، اعتماد نکرده و به جای کلیک بر روی لینک های ارسال شده به صورت مستقیم به وب سایت مربوطه مراجعه کنند.**

**- موقعیت چهارم: موزیک ها، ویدئوها و نرم افزارها**

**محیط خطرآفرین: وب سایت های دریافت (Download) موزیک، ویدئو و نرم افزار**

**سایت های دریافت (Download) موزیک، ویدئو و نرم افزار، گنجینه ای از نرم افزارهای مخرب در لباس مبدل هستند! بسیاری از متخصصان امنیتی معتقدند وب سایت های این چنینی یکی از خطرناک ترین محیط ها برای بازدید هستند. چراکه اغلب این وب سایت ها یک مدل مشخص از کسب و کار و همچنین اعتبار امنیتی کافی ندارند.**

**اگرچه بهتر است به دلیل محتوای غیرقابل اعتماد این وب سایت ها بطور کامل از بازدید آنها صرف نظر کنید اما اگر به هر دلیلی به این وب سایت ها سر زدید، بهتر است به منظور حفاظت از سیستم اصلی خود، از یک سیستم دوم با یک آنتی ویروس کاملاً بروز استفاده کنید. در نهایت فایل های دانلود شده را اسکن کرده و یکی دو روز بعد آنها را باز کنید. چراکه نرم افزارهای مخرب به محض باز شدن به همه سیستم شما رسوخ می کنند اما با تاخیر در باز کردن آنها، به آنتی ویروس اجازه می دهد مجوزهای لازم را مورد بررسی قرار دهد.**

**موقعیت پنجم: بدافزارهای پنهان در فیلم ها و تصاویر غیراخلاقی**

**محیط خطرآفرین: وب سایت های غیراخلاقی**

**سایت های نامشروع به خودی خود نسبت به سایر سایت های فعال و عمومی از درجه امنیت کمتری برخوردار هستند. اما این فرضیه تمام داستان نیست. اگرچه بازدید از این وب سایت ها به دلیل محتوای آنها، بطورکلی مخرب است اما به دلیل اینکه هیچ خط مشی امنیتی مشخصی ندارند علاوه بر محتوای مخرب می توانند حاوی برنامه های آلوده و بدافزار هم باشند. از این رو کاربران بهتر است به هیچ دلیلی به هر یک از این وب سایت ها وارد نشوند.**

**موقعیت ششم: ویدئوهای آنلاین**

**محیط خطرآفرین: وب سایت های های به اشتراک گذاری ویدئو**

**شاید برای شما پیش آمده، در حال تماشای یک ویدئوی آنلاین هشداری نمایش داده می شود مبنی بر اینکه برای دانلود این ویدئو نیازمند نرم افزار خاصی هستید. چراکه نرم افزار فعلی شما فایل مربوطه را پشتیبانی نمی کند.**

**قانونی بودن نرم افزار معرفی شده به اعتبار وب سایتی که شما در حال بازدید از آن هستید بر می گردد. اگر در حال تماشای ویدئو از یک وب سایت نا آشنا هستید بهتر است به پیغام داده شده اعتنا نکرده و نرم افزار را دانلود نکنید.**

**در نهایت اینکه اگرچه امروز اینترنت فاصله ها را کم و دسترسی ها را آسان کرده است اما هر لحظه از حضورمان در این فضا می تواند موقعیت مناسبی را در اختیار سودجویان قرار دهد. این شش موقعیت که مورد بررسی قرار گرفت اگرچه ممکن است خطرآفرین باشند اما تمام پهنه گسترده اینترنت را شامل نمی شوند. از این جهت به نظر می رسد تنها راه حل مطمئن برای مقابله با کلاهبردان و نفوذگران، هوشیاری کاربران و استفاده به جا از ابزارهای امنیتی مناسب است.**