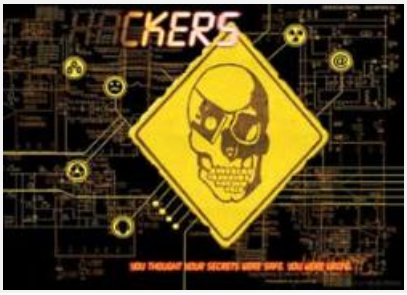

دوشنبه 19 اردیبهشت 1390 - 08:31

چگونه یک رمز عبور ایمن بسازیم

متخصصان امنیت شبکه می گویند استفاده از یک جمله برای ساخت یک رمز عبور قدرتمند بسیار کارامدتر از انتخاب یک یا دو واژه عادی و معمول است.

جام جم آنلاین: متخصصان امنیت شبکه می گویند استفاده از یک جمله برای ساخت یک رمز عبور قدرتمند بسیار کارامدتر از انتخاب یک یا دو واژه عادی و معمول است.
به گزارش مهر، این روزها هر فردی می تواند شما را تحت نظر داشته باشد، هر حرکت شما را به عنوان یک کاربر اینترنتی زیر نظر داشته و در انتظار فرصتی مناسب برای ربودن رمز عبور شما برای دسترسی به اطلاعات شخصی تان باشد.

«گراهام کلولی» مشاور ارشد شرکت امنیت نرم افزار «سوفوس» می گوید هر روز حملات سایبری جدیدی رخ می دهند و می توان روزانه در حدود 90 هزار کد مخرب را در لابراتوارها ردیابی کرد، یعنی یک کد در هر ثانیه به گفته وی انگیزه اصلی برای همه این حملات پول است، هکرها رمز عبور ایمیل کاربران را می خواهند تا بتوانند هویت کاربران را ربوده و حساب بانکی آنها را خالی کنند.

رایج ترین رمزهای عبور واژه هایی هستند که می توان آنها را درون واژه نامه یافت، از قبیل «رمز عبور»، «رومیزی» و یا حتی نام باشگاه های فوتبال.

کلولی این رمزهای عبور را بسیار بی ارزش و ناکارامد می داند زیرا به گفته وی هکرها معمولا حملات واژه نامه ای انجام می دهند و حساب ایمیل کاربران را با تمامی واژه های موجود در واژه نامه ها می سنجند تا زمانی که رمز عبور نهایی یافته شود.

هرگز از واژه های رایج و معمولی استفاده نکنید! کلولی برای پرهیز کردن از انتخاب چنین واژه هایی روشی ساده را توصیه می کند تا کاربران بتوانند از ایمن بودن رمزهای عبور خود اطمینان حاصل کرده و به راحتی آن را به یاد بیاورند اما نفوذ به آن برای هکرها دشوار باشد. از نظر وی بهترین رمز عبور برای یک کاربر «F&WL2HH&E4D» یا چیزی مشابه آن است.

شاید این رمز عبارتی به نظر بیاید که گیج کننده بوده و امکان به یاد سپردن آن وجود نداشته باشد اما کلولی می گوید این بهترین رمز عبور برای محافظت از حریم خصوصی کاربران در اینترنت است. این رمز عبور در واقع یک جمله است:«Fred And Wilma Like To Have Ham And Eggs For Dinner» (فرد و ویلیام می خواهند برای شام گوشت و تخم مرغ بخورند) در صورتی که بخواهید می توانید از نسخه فارسی این جمله نیز به عنوان رمز عبور استفاده کنید.

کلولی معتقد است می توان برای هر وب سایت از رمز عبور متفاوتی استفاده کرد به این شکل هکرها نمی توانند به سادگی به رمزهای عبور کاربران دسترسی پیدا کنند و کاربر تنها کافی است یکی از رمزهای عبور خود را به خاطر بسپارد تا بتواند تمامی آنها را در ذهن نگه دارد.

کلولی همچنین بر اهمیت به روز رسانی نرم افزاری های ویروس کش بر روی رایانه ها تاکید می کند زیرا ضعف این نرم افزارها می تواند توانایی هکرها در ربودن رمزهای عبور در حین تایپ شدن آنها توسط کاربر را افزایش دهد. به گفته وی هکرها به نرم افزارهایی به نام «جاسوس افزار» شهرت داشته و می توانند با استفاده از آن هر تک کلیدی که بر روی صفحه کلید فشرده می شود را ردیابی کنند.

جدید ترین حمله سایبری که کلولی درگیر کنترل و مهار آن شده بود حمله ای بود که با مرگ اسامه بن لادن در ارتباط بود. به گفته وی همه جهان بر روی کشته شدن بن لادن متمرکز شده بودند مردم به اینترنت رفته و به جستجوی تصاویر ویدیویی و یا عکس هایی از مرگ بن لادن می گشتند، در حالی که هکرها از این موقعیت سو استفاده کرده و به انتشار تصاویر آلوده و تقلبی اقدام کردند.

به این شکل جستجوی این محتوی در اینترنت کاربران را وارد وب سایتهایی می کرد که با هدف آلوده کردن رایانه آنها طراحی شده بود.

کلولی معتقد است همزمان با افزایش یافتن راهکارهای هکرها برای به سرقت بردن اطلاعات شخصی کاربران، کاربران نیز باید بیاموزند تا به جنگجویان سایبری تبدیل شوند، این کار را می توانید با انتخاب یک جمله به عنوان رمز عبور خود آغاز کنید!