

پس از هک شدن حساب های شخصی چه باید کرد؟



بسیاری تصور می کنند هک سیستم های رایانه ای و سرقت اطلاعات تنها به شرکت ها و سرویس های بزرگ محدود می شود و اشخاص حقیقی نیاز مبرمی برای حفاظت از رایانه یا دستگاه های دیجتالی خود در مقابله با نفوذ هکرها احساس نمی کنند اما باید گفت در مواردی اشخاص حقیقی نسبت به شرکت های بزرگ، از هک سیستم های رایانه ای و حساب های خود آسیب بیشتری می بینند.



وجود یک حفره امنیتی در نرم افزارهای نصب شده روی رایانه یا تلفن همراه، وجود برنامه های Keylogger و انواع و اقسام روش های دیگر می تواند به نفوذ هکرها به حریم خصوصی کاربران و به خطر افتادن تمامی حساب های شخصی از جمله حساب های بانکی منتهی شود.

با رعایت تمام اصول امنیتی، احتمال نفوذ هکرها کمتر خواهد شد اما هرگز از بین نمی رود. از سوی دیگر، پروسه حفاظت از حساب های شخصی تنها به کاربران محدود نمی شود و تا به امروز بارها خبرهایی از افشا شدن اطلاعات و کلمه های عبور کاربران سرویس های بزرگ با هک

شدن سرورهای آنها شنیده ایم. با این وجود در صورت هک شدن حساب های شخصی چه باید کرد و راه های جلوگیری از تبعات آن چیست؟

واکنش سریع با استفاده از یست الکترونیکی

اگر برخی از حساب های اینترنتی شما هک شده و با تغییر کلمه عبور توسط هکر، امکان ورود به آنها وجود ندارد، امید خود را از دست ندهید؛ زیرا در صورت واکنش سریع احتمال بازگرداندن حساب های از دست رفته همچنان وجود دارد.

در هنگام ثبت نام در سرویس های اینترنتی، آدرس پست الکترونیکی خود را ثبت کرده اید و در صورتی که این آدرس از دسترس هکرها در آمان مانده باشد، می توان از آن برای بازگرداندن کلمه عبور استفاده کرد.

این اقدام نخستین گام در مقابله با نفوذ هکرها و بازیابی حساب های از دست رفته محسوب شده و توصیه می شود هر چه زودتر به استفاده از آن اقدام کنید.

در زمان ثبت نام سرویس های ایمیل نیز از شما درخواست می شود به شکل دلخواه آدرس دیگری را به عنوان پست الکترونیکی پشتیبانی معرفی کنید. همواره از این پیشنهاد برای مقابله با هک شدن ایمیل خود و بازیابی کلمه عبور در آینده، بهره بگیرید.



اسکن کامل رایانه

دومین گام، جلوگیری از دسترسی های بعدی و نفوذ مجدد هکرها به اطلاعات شخصی خواهد بود که برای انجام این کار ابتدا باید حرفه

امنیتی یا راه نفوذ هکرها را پیدا کنید. برای انجام این کار باید از یک نرم افزار آنتی ویروس و ضد بدافزار برای اسکن کامل رایانه یا تلفن همراه استفاده کنید.

در این مرحله باید از ضد بدافزار و آنتی ویروس هایی کمک بگیرید که مورد تایید کارشناسان بوده و از اعتبار و قدرت کافی در زمینه کاری خود برخوردار باشند. ورود یک تروجان یا نصب Keylogger روی رایانه می تواند به ثبت اطلاعات ورودی و ارسال آنها به هکرها منجر شود و آنتی ویروس های قدرتمند قادر به تشخیص بدافزارها و حذف آنها خواهند بود.

اطلاع از مسیر بدافزارها و ویروس های پیدا شده می تواند به یافتن ریشه آلودگی و رفع آن نیز کمک کند. یک فایل دانلود شده، داده های آپلود شده توسط سایت یا نرم افزارهای بی نام و نشان، همه به نوبه خود می توانند منشأ آلودگی و راه نفوذ هکرها باشند.



نفوذ هکرها به منبع اطلاعات

همان طور که گفته شد، نفوذ هکرها به حساب های شخصی افراد تنها به بی احتیاطی اشخاص حقیقی و کاربران اینترنت مربوط نمی شود. در مواردی هکرها به سرورهای سرویس های بزرگ نظیر یاهو یا جی میل نفوذ می کنند و حجم انبوهی از اطلاعات محرمانه و شخصی افراد را به سرقت می برند.

حتی اگر تمام نکات امنیتی را رعایت کنید، ممکن است سرویس مورد استفاده شما در ابعاد بزرگ مورد دستبرد هکرها قرار بگیرد و در این حالت هیچ کاری از دست کاربران معمولی برنخواهد آمد. برای اطلاع از این گونه اتفاقات باید روی اینترنت نام سرویس خود را با عبارت Password Leak جستجو کنید و با پیگیری اخبار مرتبط مطلع شوید آیا واقعا سرویس مورد استفاده شما با سرقت اطلاعات محرمانه توسط هکرها مواجه شده است یا خیر.

برای نمونه در جولای سال ۲۰۱۲ سرویس پست الکترونیکی یاهو، هک و میلیون ها کلمه عبور کاربران این سرویس جهانی در فضای اینترنت پخش شد. با این اتفاق سایر حساب های افراد مانند حساب فیس بوک یا تویتر آنها نیز با خطر مواجه شد و مقابله با این مشکل کاملاً خارج از قدرت کاربران بود.

اوضاع زمانی بدتر می شود که از یک کلمه عبور یکسان برای تمامی حساب های خود استفاده کرده باشید و با فاش شدن آن، تمامی حساب های تان به راحتی در دسترس هکرها قرار بگیرند. برای مقابله با این مشکل توصیه می شود از کلمه های عبور مختلف برای حساب های اینترنتی متفاوت خود بهره بگیرید و به منظور مقابله با فراموش کردن آنها از برنامه های مدیریت کلمه عبور استفاده کنید.

منبع: هفته نامه عصر ارتباط

روش های برقراری امنیت رمز عبور



۸ نکته مهم برای امنیت بیشتر رمز عبور

معمولا اکثر کسانی که از کامپیوتر استفاده می کنند، رمز عبورهای خیلی ساده را انتخاب می کنند. به نظر من این یک نوع سهل انگاری است. چون رمز عبورهای خیلی ساده و خیلی معمولی در مدت زمان چند ثانیه هک می شوند. اطلاعات شخصیتان مثل شماره حساب بانکی و یا شماره کارت اعتباریتان در اختیار هکرها قرار می گیرد و به راحتی می توانند با کارت اعتباریتان خرید کنند و یا از حسابتان پول برداشت کنند.

پس برای امنیت بیشتر رمز عبور ، مقاله زیر را به دقت مطالعه نمائید :

۱- اصلا برای پسورد از اسم استفاده نکنید، چه اسمتان چه فامیلیتان یا اسم مورد علاقه و یا هر اسم خاص دیگری. چون هکرها از برنامه های فرهنگ لغات خاصی استفاده می کنند که می توانند در عرض چند ثانیه پسوردهایتان را هک کنند.

۲- برای پسوردتان، از ترکیبی از حروف بزرگ و کوچک و یا اعداد و یا علامت های خاصی استفاده کنید. البته از علامت های خاص به تنهایی استفاده نکنید. مثلاً علامت خاص همراه با عدد و یا همراه با حروف را انتخاب کنید. بیشتر کاربران از علامت ! به همراه اسمشان استفاده می کنند که به راحتی قابل هک است.

۳- برای پسورد، حروف و اعدادی را که کنار هم قرار دارند انتخاب نکنید. مثلاً پسوردهایی مثل "ghjkl" و یا "zxcvb" و یا اعداد "۱۲۳۴۵۶۷" به راحتی قابل دسترس برای هکرها هستند.

۴- برای پسوردتان، حداقل از ۸ کاراکتر استفاده کنید. برای پسوردهایی که از ۴ کاراکتر تشکیل شده اند، حدود ۴۵۰۰۰ حالت وجود دارد، ولی برای پسوردهایی که از ۸ کاراکتر و علامت های خاص تشکیل شده اند، در حدود یک میلیارد حالت وجود دارد.

PASSWORD

۵- پسوردتان را همواره تغییر دهید. اگر زمان استفاده از پسوردتان طولانی شود احتمال هک شدن پسوردتان بیشتر است. بهتر است که هر ۳ ماه یک بار پسوردتان را تغییر دهید.

۶- پسوردتان را به هیچ کس ندهید. اگر کسی از شما به هر طریقی پسوردتان را خواست، به او ندهید! هکرها معمولاً خودشان را به عنوان یکی از کارکنان شرکت های بزرگ، یا سرویس کار کامپیوتر معرفی می کنند و یا توسط تلفن و یا ایمیل، پسوردتان را برای حل کردن مشکلاتان از شما می خواهند. ولی این نکته را فراموش نکنید که هیچ شرکت معتبری از شما پسورد نمی خواهد.

۷- تا حدی که امکان دارد پسوردتان را در جایی ننویسید. اگر روی یک کاغذ آن را بنویسید و آن را در جای امنی مثل کیفتان قرار دهید، باز هم امکان هک شدنش وجود دارد. یا کاغذ را روی مانیتور یا هر جای دیگری نچسبانید و یا زیر کیبورد یا پد ماوس و یا هر جای دیگری که در معرض دید باشد نگذارید.

۸- پسوردتان را در کامپیوتر ذخیره نکنید. کامپیوتر می تواند پسوردتان را ذخیره کند تا شما مجبور نباشید هر

دفعه که می خواهید وارد شوید پسوردتان را بزنید. به این ترتیب اگر که مرتبا می خواهید وارد شوید احتیاج ندارید که پسورد را هر بار وارد کنید، این باعث می شود که خیلی زود پسورد را فراموش کنید. این نکته را یادتان باشد که اگر بخواهید پسورد را عوض کنید، باید حتما پسورد قبلی یادتان باشد.



۷ تکنیک ایجاد رمز عبور حرفه ای با امنیت بالا

- ۱- برای ایجاد کردن پسورد، از حروف بزرگ و کوچک به صورت یک در میان یا دو در میان استفاده کنید. مثل: InTeRnEt و INtErNet
- ۲- یک جمله را در ذهن خود در نظر بگیرید. حرف اول کلمات این جمله را برای پسوردتان انتخاب کنید. مثلا: "Man Har Ruz Be Site Amoozesh Computer Sar Mizanam" پسورد من : "MHRBSACSM"
- ۳- اسم خودتان یا یک لغت را در نظر بگیرید، حالا حروف سمت راست یا چپ آن را که روی کیبورد است برای پسوردتان انتخاب کنید. مثلا: COMPUTER پسورد من است و حروف سمت راست آن : pdysfroy
- ۴- عدد یا تاریخی برای خودتان انتخاب کنید و سپس بر طبق آن دکمه Shift را نگهدارید و تایپ کنید. مثلا: ۶۹۲۵۱۳۶۸ که می شود: (^>%@>^*#!
- ۵- در پسوردتان از علامت های خاص استفاده کنید. مثال: C/om\@p{u\$t%er*&
- ۶- لغات یک جمله را به اختصار بنویسید. این اختصارات مربوط به خودتان است و قاعده و قانون خاصی ندارد. جمله: "I have a best site for my lessons" پسورد: ihvbstsfrmls
- ۷- لغت یا ترکیبی از لغات و اعداد را برای خود انتخاب کنید. بعد آن را به هم بریزید مثلا حرف اول را به جای حرف آخر قرار دهید و یا جای اعداد را با حروف را با هم عوض کنید. مثال: ut36ter410comp319:پسورد com319put410er36

منبع: <http://www.amoozesh-computer.ir/security/password-scurity>