**چگونه هک نشویم؟**

**وقتی که سازمانهای دولتی، افراد مشهور و حتی سازمانهای نظامی هک می شوند، پس احتمال هک شدن شما هم وجود دارد. در اینجا چند شیوه برای حفظ امنیت در حالت آنلاین از سوی کاربری به نام مین سالکین" Miné Salkin "ارائه شده است که خود بارها و بارها هک شده و تجربه اندوزی کرده است.**

**وقتی که سازمانهای دولتی، افراد مشهور و حتی سازمانهای نظامی هک می شوند، پس احتمال هک شدن شما هم وجود دارد. در اینجا چند شیوه برای حفظ امنیت در حالت آنلاین از سوی کاربری به نام مین سالکین" Miné Salkin "ارائه شده است که خود بارها و بارها هک شده و تجربه اندوزی کرده است.این کاربر با تجربه توصیه های زیر را ارائه کرده است:

محیط های کاری خود را به طور مرتب تجدید کنید؛ تاریخ انقضا را فاش نکنید

با گذشت چهار سال از مدیریت وبسایت، من اشتباه کرده و محیط کار را به موقع تجدید نکردم و آنها را آن را به فروش رساندند. وقتی من به وبسایت خود رفتم، دیدم که یک شرکت در شرق اروپا آن را خریده است. اکنون، وبسایت خبری حرفه ای من تبدیل به یک چت روم و سرگرمی شده است.

من و وکیلم یک نامه گزارش تخلف آماده کرده و فوراً آن را ارسال کردیم. جالب بود که من می توانستم این دامنه را به قیمت معقول دوباره خریداری کنم. آنهامتین و مؤدب بودند و در این زمینه، باید اعتراف کنم که من خیلی خوش شانس بودم.

به لحاظ فنی این مورد هک به شمار نمی آید، اما من توصیه های کارشناسی خود را منتشر می کنم.

حساب های قدیمی در رسانه های اجتماعی را حذف کنید

چند ماه بود که دوستانم پیام هایی برای من ارسال می کردند که حساب من در snapchat هک شده است. من پیش خودم فکر می کردم که آیا این امکان پذیر است؟ من متوجه شدم که از حساب کاربری من برای فروش قرص های رژیمی جادویی استفاده می شود. من که مقداری اضافه وزن دارم، احساس کردم که به من بی احترامی و توهین شده است. من این موضوع را به مدیریت سایت اطلاع داده و حساب کاربری خود را حذف کردم. بعد از این کار، که احساس شجاعت و کارآگاه بودن می کردم، آدرس آی پی مورد نظر را ردگیری کرده و متوجه شدم که مطعلق به روسیه است اما می ترسیدم هر گونه تماسی برقرار کنم.

هر حساب کاربری غیرفعالی که شما دارید، به منزله دعوتنامه ای برای هکرها است که حضور شما در رسانه های دیجیتال را اشغال کنند. مدتهاست که از حساب خود استفاده نکرده اید؟ خود را از آن رها کنید. قبل از اینکه گذرواژه خود را فراموش کنید، یا امکان وصل شدن را از دست بدهید، از دست آنها رها شده و مطمئن شوید که حسابتان مسدود شده است. کسی نمی داند که احتمالاً شخصی در حال استفاده از نام شما برای شکار یک قربانی بی خبر است. شما باید هر از چندگاهی تصویر پروفایل خود را در گوگل جستجو کنید تا مطمئن شوید کسی این کار را با شما نکرده است.

راهبرد گذرواژه

وقتی چند سال پیش گذرواژه ایمیل من هک شد، برای من خیلی عجیب بود. هکر یک ایمیل جمعی برای دوستان و خانواده من ارسال کرده و بیان کرده بود که در اسکاتلند هستم و گذرنامه ام را گم کرده ام و برای دریافت گذرنامه جدید از سفارت، نیاز به پول دارم. موضوع جالب اینجا بود که شیوه نگارش هکر شبیه شیوه من بوده و من ماه گذشته به آن منطقه سفر کرده بودم.

راه هایی برای بهبود راهبرد گذرواژه

1-    گذرواژه پیچیده انتخاب کنید. ترکیبی از علائم نگارشی و اعداد و کلمات نامفهوم و بی معنی.

2-    از تأیید دو مرحله ای استفاده کنید.

3-   برای هر حساب خود، گذرواژه مجزا تعیین کرده و آنها را به هم لینک نکنید.

4-    گذرواژه خود را روی یک تکه کاغذ نوشته و آن را در جای امن نگهداری کنید. این بهترین شیوه برای حفظ گذرواژه است.

5-    تمام گذرواژه های حساب های خود را مرتباً بروزرسانی کنید؛ حد اقل دو بار در سال.

امروزه باید راهبرد گذرواژه به عنوان یک درس در مدارس ابتدایی تدریس شود زیرا موضوع مهمی است، درست مثل دوش گرفتن روزانه یا رفتن به مدرسه یا محل کار.

متأسفانه هیچ روش مؤثری برای حفظ کامل امنیت در حالت آنلاین وجود ندارد. حتی اگر از یک آژانس امنیبی بزرگ استفاده کنید، بیشترین خدماتی که به شما ارائه می شود این خواهد بود که بعد از وقوع آسیب، آن را کم کنند. تمام سعی خود را به کار ببرید تا همیشه در رأس آن باشید.**

**منبع :** **http://www.cyberpolice.ir**

[**پایگاه خبری تحلیلی انتخاب (Entekhab.ir)**](http://khabarfarsi.com/ext/13588333)