چگونه از این اتفاق جلوگیری کنیم

چگونه هکرها بدون رمزعبور وارد شبکه اجتماعی شما می‌شوند + راه‌حل

سوال مهمی که این روزها بر سر زبان‌ها افتاده این است که هکرها چگونه می‌توانند بی آن‌که نیازی به گذرواژه‌ها داشته باشند به حساب‌های کاربری وارد شوند. اما سوال بدیهی‌تر این است که چگونه می‌توانیم اطمینان حاصل کنیم که این اتفاق برای ما رخ نخواهد داد؟

در ساعات اولیه چهارشنبه هفته گذشته بود که یکی از میزبان‌های حساب‌های توییتری در معرض تهدید قرار گرفت. بله درست شنیده‌اید. اکنون سوال مهمی که بسیاری از کاربران مطرح می‌کنند این است که چگونه باید مطمئن شویم که ما از خطر نفوذ در امان خواهیم بود و از چه راهکارهایی باید برای بستن درب‌های پشتی که ممکن است به دیگران اجازه دهد به حساب‌های ما وارد شوند استفاده کنیم.

حساب‌های حرفه‌ای و معتبری همچون دانشگاه دوک، فوربس و سازمان عفو بین‌الملل به احتمال زیاد از تدابیر امنیتی بسیار قدرتمندی همچون احرازهویت دو عاملی و گذرواژه‌های قدرتمند استفاده می‌کنند. کاربران عادی نیز می‌توانند از چنین سازوکارهای مهم حفاظتی برای مصون نگه داشتن خود از خطرات استفاده کنند. اما نکته‌ای که باید به آن توجه داشته باشید این است که این اقدامات به تنهایی کافی نیست. به واسطه آن‌که هکرها از راهکارهای هوشمندانه‌تری برای نفوذ استفاده می‌کنند. مهم‌ترین راهکاری که بسیاری از کاربران توجه اندکی به آن دارند، مجوزهای نرم‌افزاری است.

مطلب پیشنهادی

استفاده بهتر از تلگرام با یادگیری ترفندهای کاربردی این اپلیکیشن پیام‌رسان
ترفندهای جالب تلگـرام که بهتر است آن‌ها را بدانید (بخش اول)

اگر برای ورود به یک برنامه کاربردی یا سرویسی به جای آن‌که یک نام کاربری یا گذرواژه‌ای را ایجاد کنید، از طریق حساب‌های موجود در شبکه‌هایی همچون فیسبوک، توییتر یا گوگل استفاده کنید به راحتی یک حفره "مجوز نرم‌افزاری" را به وجود آورده‌اید. ورود به برنامه‌های کاربردی از طریق حساب‌ها ویژگی خوبی است. این ویژگی به شما اجازه می‌دهد در مورد گذرواژه‌ها و گاهی اوقات برنامه‌های کاربردی نگرانی کمتری داشته باشید. به واسطه

آن‌که به طور مستقیم به آن‌ها وارد می‌شوید، اما در مقابل مسئولیت مشکلات امنیتی آن‌را نیز باید قبول کنید.

در نمونه مشابهی برنامه‌ای موسوم به Twitter Counter که به نظر می‌رسد دارای یک نقص بوده مورد هک قرار گرفت. این برنامه به این منظور طراحی شده بود تا به کاربران اجازه دهد به تحلیل داده‌های حساب‌های کاربری خود بپردازند. برنامه Twitter Counter به یک مجوز نیاز داشت. اما این مجوز تنها به منظور دسترسی به داده‌ها مورد استفاده قرار نمی‌گرفت. این مجوز به برنامه فوق اجازه می‌داد به توییتر نیز دست پیدا کند. این رویکرد در نوع خود خرابکارانه نیست، به دلیل این‌که به شما اجازه می‌داد به طور مستقیم از درون این برنامه توییت‌هایی را انجام دهید. اما اگر این برنامه در معرض تهدید قرار گیرد (که به نظر می‌رسد این اتفاق رخ داده است) به هکرها اجازه می‌دهد از طریق دسترسی به حساب کاربری شما توییت‌های خرابکارانه‌ای را ارسال کنند.

مطلب پیشنهادی

مشکل پردازنده‌ها برای مالکان آن‌ها
ویندوزهای قدیمی روی سخت‌افزارهای جدید دیگر به‌روزرسانی نمی‌شوند

نفوذ به واسطه یک درب پشتی

در حالت کلی میزان دسترسی این برنامه‌ها به حساب‌ها محدود است. این برنامه‌ها قادر نیستند گذرواژه شما را به آن چیزی که دوست دارند تغییر داده یا حساب‌های ساخته شده در فیسبوک، توییتر یا گوگل را به شکل معکوس مورد استفاده قرار دهند. این برنامه‌ها هیچ‌گاه گذرواژه واقعی شما را به دست نمی‌آورند. به واسطه آن‌که حساب اصلی شما به سادگی با تولید یک توکن (token) از شما محافظت می‌کند.

برنامه‌هایی این چنینی زمانی که موفق نشوند از درب اصلی (گذرواژه اصلی) به ساختمان وارد شوند، از درب پارکینگ (حساب‌های شبکه‌های اجتماعی) وارد خواهند شد. دربی که کلید ورود به آن‌را شما از طریق حساب‌هایی که در شبکه‌های اجتماعی ساخته‌اید و از طریق آن‌ها به این برنامه‌ها وارد شده‌اید در اختیارشان قرار داده‌اید.

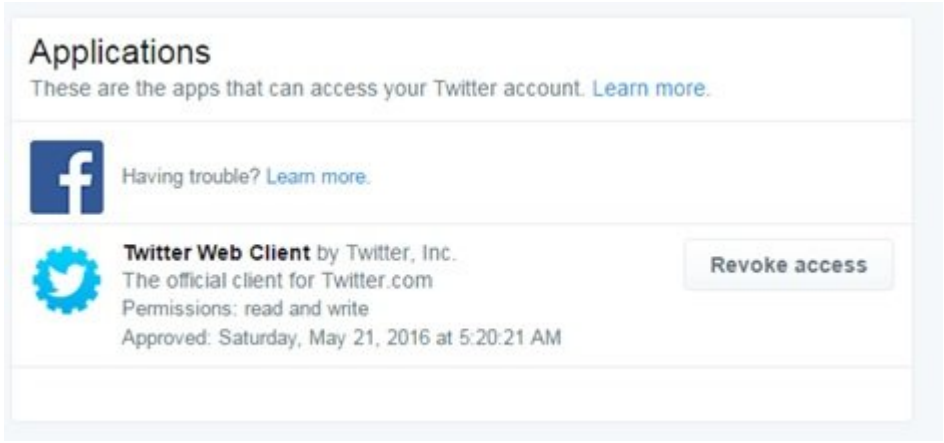
مطلب پیشنهادی

بزرگ‌ترین حمله بدون نیاز به گذرواژه
چگونه هکرهای روسی بدون گذرواژه به میلیون‌ها حساب کاربری یاهو دسترسی پیدا کردند

راهکار دفاعی چیست؟

اما راه‌حل چیست؟ ابتدا سعی کنید مجوزهای مختلفی که به این برنامه‌ها تخصیص داده‌اید را لغو کرده یا حداقل هر چند ماه یکبار این مجوزها را مورد بازبینی قرار دهید. هر حسابی به شیوه مختلف و به برنامه‌های کاربردی مشخصی اجازه می‌دهد به حساب شما دست پیدا کنند. کافی است یک دقیقه وقت بگذارید و فهرستی از مواردی که به آن‌ها نیازی ندارید یا به آن‌ها اعتماد ندارید را آماده کرده و آن‌ها را حذف کنید.

توییتر

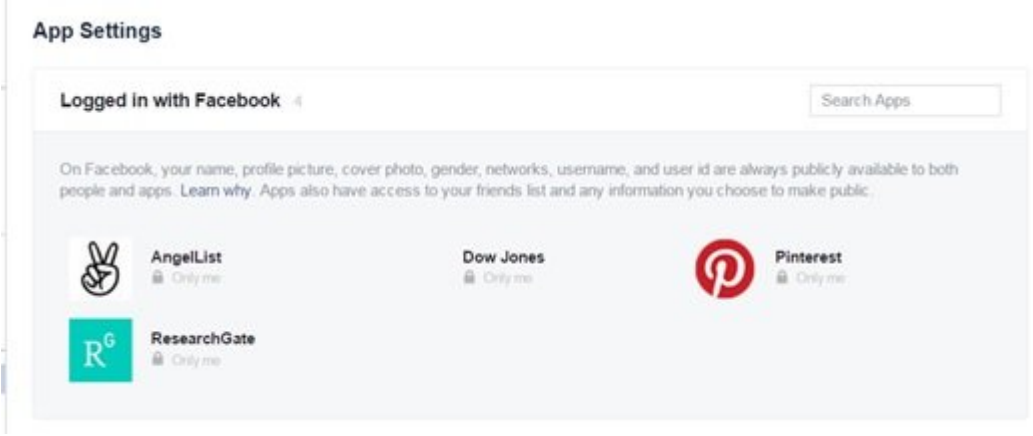


روی نماد تصویر خودتان که در سمت راست حساب در کنار دکمه Twitter قرار دارد کلیک کرده و گزینه Settings and privacy را انتخاب کنید. در سمت چپ صفحه روی گزینه Apps کلیک کنید. در ادامه فهرستی از برنامه‌های کاربردی را مشاهده می‌کنید. در مقابل هر برنامه گزینه Revoke Access وجود دارد. با کلیک روی این گزینه فهرستی از مجوزهای تخصیص یافته به برنامه‌ها را مشاهده خواهید کرد.

گوگل

گوگل به سادگی از طریق گزینه Security Checkup این قابلیت را در اختیار شما قرار می‌دهد. این گزینه به طور خودکار مواردی همچون مجوز برنامه‌های کاربردی، گذرواژه‌های ویژه، دستگاه‌های متصل شده و دیگر آسیب‌پذیری‌های حساب کاربری شما را بررسی می‌کند. بهتر است همین حالا این‌کار را انجام دهید و حساب خود را تمیز کنید.

فیسبوک



روی منوی بازشو که در کنار علامت سوال در سمت راست صفحه قرار دارد کلیک کرده و گزینه Settings را انتخاب کنید. در صفحه ظاهر شده در سمت چپ صفحه روی گزینه Apps کلیک کنید. در صفحه ظاهر شده فهرستی از برنامه‌هایی که قادر هستند از حساب فیسبوک شما استفاده کنند را مشاهده می‌کنید. بهتر است برای برنامه‌های کاربردی گزینه read-only را انتخاب کنید. این گزینه به برنامه‌های کاربردی اجازه می‌دهد تنها به داده‌های شما دسترسی داشته باشند بدون آن‌که قادر به انجام کار دیگری باشند.

برای حساب‌های دیگری که از مکانیزم یکپارچه شدن با برنامه‌های کاربردی پشتیبانی می‌کنند فهرست‌های مشابهی وجود دارد که به راحتی می‌توانید آن‌را پیدا کنید. اما این نکته را فراموش نکنید شما ممکن است با تخصیص مجوز به برنامه‌های کاربری به طور ناخواسته امنیت خود را در معرض خطر قرار دهید. در نتیجه بهتر است پیش از به کارگیری برنامه‌های کاربردی به دقت موافقت‌نامه‌های آن‌ها را مطالعه کنید.

تاریخ انتشار:
02 فروردین 1396

نشانی منبع: https://www.shabakeh-mag.com/security/7293