شبکه اجتماعی ما چگونه هک می‌شود؟

مجرمان سایبری سعی می‌کنند هنگام نفوذ به حساب‌های بانکی، تلفن‌ها و رایانه‌های شخصی هیچ ردی از خود باقی نگذارند اما اگر شخصی وارد شبکه‌های اجتماعی و حساب ایمیل شما شود، علائم هشداردهنده‌ای در این زمینه وجود دارند. اینکه شخص دیگری به شبکه‌های اجتماعی شما دسترسی داشته باشد نگران کننده است و هکرها بدون گذاشتن رد پا از تکنیک‌های مختلف برای این کار استفاده می‌کنند. اکنون راه‌هایی وجود دارد که با استفاده از آنها می‌توانید از وجود نفوذی‌ها باخبر شوید، اینها شامل دیدن محتوای متفاوت از آنچه قبلاً به آن عادت داشتید در تایم لاین یا عدم دریافت اعلان در تلفن است. در پاسخ به هرگونه فعالیت مشکوک حساب، باید رمز عبور خود را روی حروف، اعداد و کاراکترهای تصادفی بازنشانی کنید. در برخی موارد ممکن است دستگاه شما (مانند رایانه شخصی) به دلیل سرقت اطلاعات بدافزار در معرض خطر قرار گیرد، در این صورت اجرای اسکن آنتی ویروس بسیار مهم است. اینها نشانه‌هایی هستند که باید مراقب آنها باشید:

محتوایی که در شبکه‌های اجتماعی می‌بینید تغییر می‌کند

اگر ناگهان محتوای ناآشنا در شبکه‌های اجتماعی دیدید یا محتوایی به زبان‌های جدید، می‌تواند نشانه‌ای از حضور شخصی در حساب شما باشد. بنابراین نسبت به تغییرات محتوایی که در شبکه‌های اجتماعی می‌بینید هوشیار باشید.
تغییرات ناگهانی، مانند هجوم پست‌ها به زبان‌های ناآشنا یا پیشنهادات از حساب‌هایی که با آن‌ها درگیر نشده‌اید، می‌تواند نشان‌دهنده فعالیت مشکوک باشد، زیرا الگوریتم‌های شبکه‌های اجتماعی بر اساس ترجیحات شما تنظیم شده‌اند و تغییرات غیرمنتظره ممکن است به معنای دسترسی غیرمجاز باشد.

شما پیام دریافت می‌کنید، اما هیچ اعلانی نمی‌آید

اگر می‌بینید پیام‌هایی در حساب‌تان ظاهر شده، اما اعلان‌های معمول را روی تلفن‌تان دریافت نمی‌کنید، یک علامت هشدار است که شخص دیگری ابتدا آنها را می‌بیند.
هکر می‌تواند قوانینی را در صندوق ورودی شما تنظیم کند تا پیام‌های خاصی را تغییر دهد بنابراین آنها می‌توانند حساب‌های بیشتری از جمله حساب‌های بانکی را در معرض خطر قرار دهند.
در صورت مشاهده ایمیل‌های جدید و خوانده نشده بدون دریافت اعلان‌های مربوطه و تاخیر در تحویل، مراقب باشید. این می‌تواند نشانه‌ای باشد که هکرها قوانینی را وضع کرده‌اند که ایمیل‌ها را از صندوق ورودی شما مخفی کند. هکر ممکن است به طور انتخابی پیام‌های خاصی را منتشر کند در حالی که بقیه را پنهان می‌کند.
در اینصورت تنظیمات صندوق ورودی خود را بررسی کنید تا ببینید آیا قوانینی برای هدایت ایمیل‌ها به آدرس‌هایی که نمی‌شناسید وجود دارد یا خیر.

تراکنش‌های بسیار کوچک در بانکداری آنلاین شما اتفاق می‌افتد

هدف اکثر هکرها دریافت پول است. به محض اینکه در یک حساب ایمیل قرار گرفتند، سعی می‌کنند اقداماتی از جمله به خطر انداختن حساب‌های بانکی را انجام دهند. حتی هزینه‌های ناشناخته کوچک می‌تواند یک علامت هشدار باشد.
به طور مرتب صورتحساب‌های بانکی یا کارت اعتباری را برای تراکنش‌های غیرمجاز بررسی کنید. هکرها ممکن است برای آزمایش قبل از اقدام به تراکنش‌های بزرگ‌تر، تراکنش‌های کوچک را آغاز کنند.
حتی مراقب مبالغ به ظاهر ناچیز باشید و هرگونه تراکنش مشکوک را فورا به بانک خود گزارش دهید.

یک بنر زرد رنگ زیر ایمیل شما ظاهر می‌شود

در جیمیل روی دسکتاپ، بنر زرد رنگی را مشاهده خواهید کرد که نشان می‌دهد شخصی از مکانی ناآشنا وارد سیستم شده است.
اکثر سرویس‌های آنلاین گزارش‌های فعالیت را ارائه می‌کنند که به شما امکان می‌دهد ورود به سیستم را نظارت کرده و به شناسایی دقیق هکرها کمک می‌کند.
به طور منظم گزارش‌های فعالیت ارائه شده توسط سرویس‌ها را برای نظارت بر زمان ورود به سیستم و آدرس‌های IP بررسی کنید.
فعالیت‌های غیرمعمول را بررسی کنید، جلسات ناشناخته را لغو کنید (همچنین می‌توانید از همه دستگاه‌هایی که وارد سیستم شده‌اید درخواست خروج از سیستم را بدهید). به یاد داشته باشید، دستگاه‌های در معرض خطر ممکن است منجر به خطر انداختن حساب کاربری شما شود.

حساب شما مسدود شده است

یک علامت هشدار کلیدی در مورد فعالیت‌های مخرب این است که حساب کاربری شما به طور ناگهانی به حالت تعلیق درآمده یا لغو شود. بنابراین مراقب تعلیق غیرمنتظره حساب باشید، اگر اعلان‌هایی درباره تعلیق حساب دریافت می‌کنید، ممکن است نشان‌دهنده فعالیت‌های مخرب باشد. برای بررسی و رفع مشکل فوراً با ارائه دهندگان خدمات تماس بگیرید. اگر ناگهان از سیستم خارج شدید، این می‌تواند یک علامت هشدار نیز باشد. اگر متوجه شدید که بارها و بارها بدون شروع از سیستم خارج شده‌اید، تلاش‌های مشکوک برای ورود به سیستم را بررسی کنید.
جلسه‌های فعال، دستگاه‌های مورد اعتماد و لیست دستگاه‌های ورود به سیستم را بررسی کنید و اگر چیزی مشکوک به نظر می‌رسد، دسترسی را لغو، رمز عبور خود را تغییر دهید و بررسی کنید که احراز هویت چند مرحله‌ای تنظیم شده و به درستی کار می‌کند.

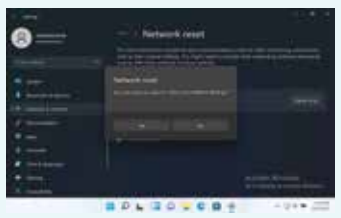
ویندوز

ریست تنظیمات شبکه در ویندوز ۱۱

اگر با مشکلات ارتباطی زیادی دست و پنجه نرم می‌کنید، احتمالا زمان آن رسیده که تنظیمات شبکه را در ویندوز ۱۱ ریست کنید. البته در اکثر مواقع پیش از چنین کاری، باید روش‌های دیگر را امتحان کنید اما اگر هیچ‌کدام از آنها کاربردی برای‌تان نداشتند، باید تنظیمات شبکه را ریست کنید.

برای ریست کردن تنظیمات شبکه در ویندوز ۱۱ مراحل زیر را دنبال کنید:

۱



به تنظیمات ویندوز بروید. برای این کار در نوار جست‌وجوی منوی استارت، Settings را تایپ کرده و بهترین گزینه مطابق با آن را انتخاب کنید. البته می‌توانید به جای چنین کاری، از کلیدهای ویندوز و I هم استفاده کنید.
حالا از سمت چپ گزینه Network & Internet را انتخاب کنید.
در ادامه به سمت پایین اسکرول کرده و برای ریست شبکه، گزینه Advanced network settings را بزنید.
در بخش More settings در Advanced network settings، گزینه Network reset را انتخاب کنید.
در نهایت روی گزینه Reset now کلیک کنید.

۲

نحوه تغییر تنظیمات DNS در ویندوز ۱۱

برای تغییر DNS در ویندوز ۱۱ مراحل زیر را انجام دهید:
با کلیدهای Win + I به تنظیمات ویندوز رفته و گزینه Network & Internet را انتخاب کنید.
در ادامه روی Advanced network settings کلیک کنید.
در اینجا، روی آداپتور شبکه موجود زیر بخش Network Adapters کلیک کنید. برای مثال اگر از ارتباط اترنت استفاده می‌کنید، آن را انتخاب کنید. چنین کاری را برای اتصال وای‌فای هم می‌توانید انجام دهید.
روی گزینه View additional properties کلیک کنید.
حالا دکمه Edit در مقابل اختصاص DNS سرور را بزنید.
زیر بخش Edit DNS Settings، روی Manual کلیک کرده و سپس تنظیمات IPv۴ یا IPv۶ را انتخاب کنید.

کلودفلر: ۱.۱.۱.۱ و ۱.۰.۰.۱
گوگل: ۸.۸.۸.۸ و ۸.۸.۴.۴