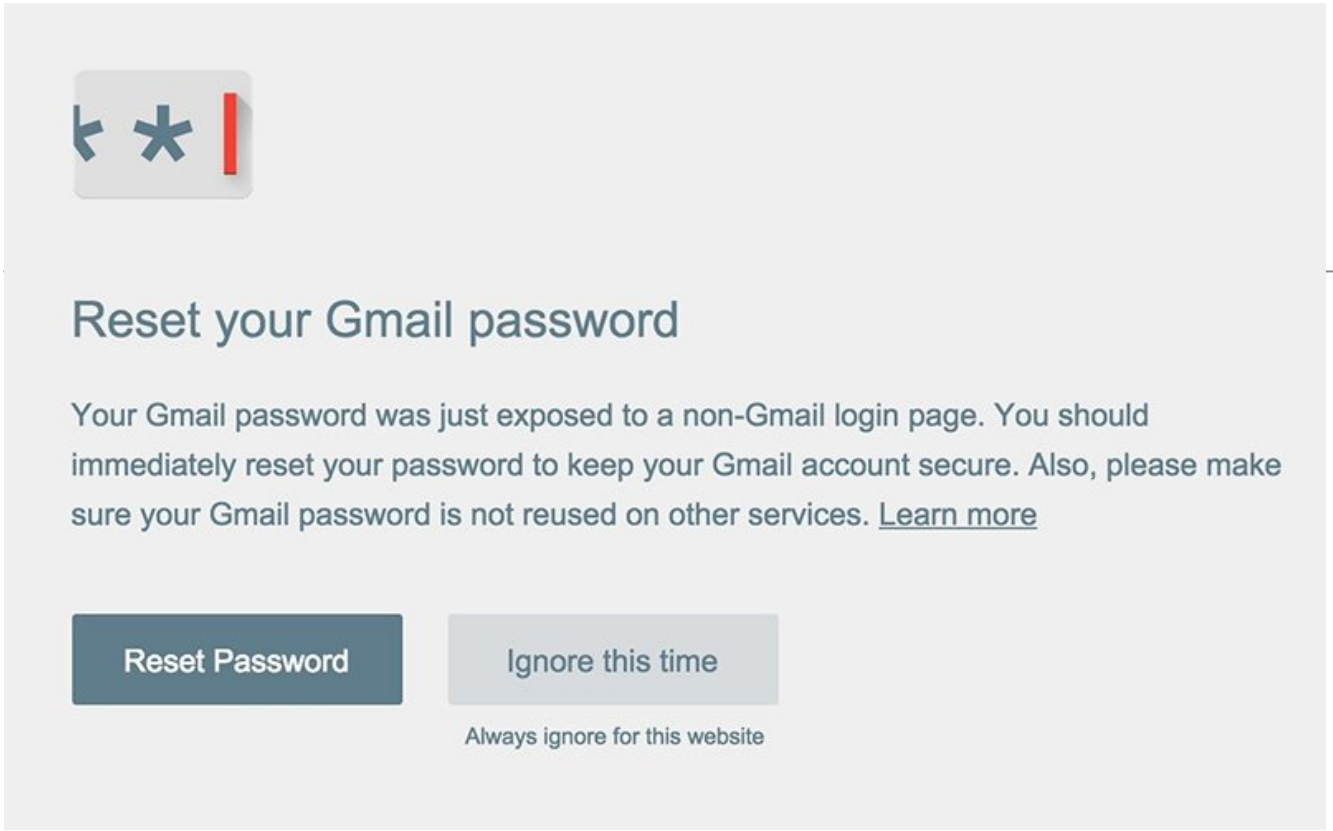
افزونه امنیتی قربانی شده

سیستم هشدار فیشینگ گوگل خود قربانی حمله فیشینگ شد



گوگل ابزار امنیتی ویژه‌ای را برای مبارزه با حمله‌های فیشینگ طراحی کرد. این افزونه رایگان که برای مرورگر کروم طراحی شده است، Password Alert نام دارد. اما تنها یک روز برای قربانی شدن افزونه مرورگر کروم لازم بود که برای مقابله با تهدیدات طراحی شده بود.

پل مور، مشاور امنیت اطلاعات، در ویدویی که اول ماه می منتشر کرد، نشان داد چگونه سیستم هشدار گذرواژه گوگل با اضافه کردن تنها هفت خط کد ممکن است به فریب سایت‌ها بپردازد. این ابزار به گونه‌ای طراحی شده است که وقتی کاربران روی یک سایت مخرب وارد شوند، به صدا درمی‌آید و اعلام می‌کند این سایت مورد بازدید کاربر درصدد سرقت اطلاعات است؛ عملی که در دنیای امنیت به‌نام فیشینگ از آن یاد می‌شود. مور در مصاحبه‌ای می‌گوید: «به‌طور خلاصه، هر کس تصمیم دارد یک حمله فیشینگ را روی حساب کاربری گوگل اجرا کند، به‌سادگی تنها به هفت خط کد مهندسی معکوس برای بی‌مصرف کردن سیستم محافظتی هشدار گوگل نیاز دارد. این یک واقعیت خجالت‌آور است.»

بعد از اعلام این خبر توسط مور، گوگل به‌سرعت واکنش نشان داد و درو هینتز از گوگل اعلام کرد این رخنه اصلاح شده است و کاربران برای حفظ ایمنی خود و پیش‌گیری از مشکلات می‌توانند این افزونه را به‌روزرسانی کنند. Password Alert سعی می‌کند تا با جلوگیری از ورود گذرواژه‌ها به سایت‌های مختلف و استفاده مجدد آن‌ها توسط سایت‌های غیرگوگلی از آن‌ها محافظت کند. هرگاه یک گذرواژه گوگل به سایتی وارد می‌شود، Password Alert پیغامی را با این مضمون نشان می‌دهد: «گذرواژه جی‌میل شما توسط یک سایت غیرگوگلی در معرض افشا قرار دارد» و به کاربر اعلام می‌دارد گذرواژه جی‌میل خود را فوراً تغییر دهد. ایده‌ای که در پس‌زمینه Password Alert است، بر پایه پیش‌گیری از حمله‌های فیشینگ قرار دارد. فیشینگ شیوه مورد استفاده هکرها است که خود را به‌عنوان یک شرکت یا سازمان مشروع نشان می‌دهند و به سرقت اطلاعات حساس از قبیل گذرواژه‌ها، شماره تأمین اجتماعی یا شماره کارت‌های اعتباری می‌پردازند. در بیش‌تر موارد، کسانی که از حمله‌های فیشینگ استفاده می‌کنند، به بازطراحی سایت یک شرکت یا یک ایمیل موقت می‌پردازند.

در یک حمله فیشینگ، ممکن است ایمیلی را از شخصی دریافت کنید که وانمود می‌کند از گوگل است و از شما می‌خواهد تا اطلاعات و جزییات مربوط به حساب کاربری خود را در یک سایت مخرب وارد کنید. زمانی که تصمیم می‌گیرید این اطلاعات را در سایت مخرب وارد کنید، Password Alert وارد عمل شده و به شما پیغام هشداری را نشان می‌دهد که شما در حال وارد کردن اطلاعات شخصی خود در یک سایت غیرگوگلی هستید. آن گونه که مور در ویدیوی خود نشان داده، او یک صفحه جعلی لاگین گوگل را طراحی کرده است. در نگاه نخست، صفحه ساخته شده واقعی به‌نظر می‌رسد و همان صفحه اصلی جست‌وجوی این شرکت است. با این حال، این صفحه دربرگیرنده کدهای

جاوا اسکریپت از پیش ساخته‌ای است که نحوه عملکرد Password Alert را تغییر می‌دهد. این کد زمان نمایش پیغام هشدار را به 5 میلی‌ثانیه کاهش می‌دهد و عملاً امکان مشاهده آن را برای کاربر غیرممکن می‌سازد و کاربر را قربانی یک حمله فیشینگ می‌کند. در نگاه نخست، به‌نظر می‌رسید گوگل موفق شده است با اصلاح این رخنه از امنیت کاربران محافظت به عمل آورد، اما مور یک‌بار دیگر در به‌روزسانی توییت خود اعلام کرد، او رخنه دیگری در جاوا اسکریپت شناسایی کرده است که این اکسپلویت در به‌روزرسانی اخیر گوگل وجود دارد. گوگل هنوز درباره رخنه‌ای که توسط مور شناسایی شده واکنشی نشان نداده است.

تاریخ انتشار:

24 خرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/848