کد خبر: ۲۵۷۳۶۱
شنبه ۲۳ اسفند ۱۳۹۹ ۱۰:۱۲

۵ ترفند فریبنده هکرها برای بازی با روان شما&#۴۷; کلمات جادویی که شما را در اختیار سارقان مجازی قرار می دهد

در این خبر با ۵ ترفند روانشناختی که هکرها برای فریب کاربران هنگام بارگیری اطلاعات استفاده می‌کنند، آشنا می‌شوید.<br&#۴۷><br&#۴۷;>

به گزارش سایت خبری پرسون، مجرمان سایبری برای فریب کارمندان و افراد برای باز کردن، کلیک کردن و بارگیری اطلاعات از طریق ایمیل، به طرز خارق‌العاده‌ای روش‌های زیرکانه و هوشمندانه‌ای طراحی می‌کنند. این طرح های فیشینگ به منظور دستیابی به داده‌های ارزشمند شرکت یا آسیب رساندن به یک سازمان اجرا می‌شوند. شرکت‌ها به خوبی از این خطرها آگاه هستند و بسیاری از آنها سعی می‌کنند با آموزش به کارکنان خود در مورد کلاهبرداری های جدید فیشینگ و امکان فیشینگ، در رده جدیدترین برنامه‌ها قرار بگیرند.

چگونه طرح‌های فیشینگ می‌توانند اینقدر موفق باشند؟

هکرها ساده ترین راه را برای کشف اطلاعات حساس شرکت با استفاده از روشی کشف کرده اند که شامل سوءاستفاده از نقص فنی یا از طریق متوسل شدن به خشونت، تهدید یا حتی تماس شخصی نیست. آنها به سادگی از اصول اولیه مهندسی اجتماعی استفاده می‌کنند که احساسات انسانی را شکار می‌کنند. ثابت شده است که ایمیل‌هایی که باعث می‌شود قربانی هدف قرار بگیرد و احساس ترس یا احساسات شدید دیگری می‌کند، که باعث می‌شود آنها بدون فکر، عمل مورد نظر را انجام دهند، این کار معمولاً کلیک کردن روی پیوند مخرب یا باز کردن پرونده آلوده است. همانطور که بنگاه های اقتصادی تلاش می‌کنند از این حملات مهندسی اجتماعی فیشینگ جلوگیری کنند، عنصر انسانی هر بار آن‌ها را برنده خواهد کرد: طبق ۹۰ درصد TechRadar، نقض داده ها ناشی از خطای انسانی است. انسان ها ثابت کرده اند بارها ضعیف ترین حلقه در زنجیره سایبری هستند.

حالا ۵ ترفند روانشناختی برتر را که هکرها در حملات فیشینگ استفاده می‌کنند ، بررسی می‌کنیم:

ترس از هیچ چیزی وجود ندارد به جز ترس از خود

احساس ترس هنگامی فعال می‌شود که قربانی معتقد باشد اگر عمل نکند اتفاق وحشتناکی رخ خواهد داد. خطر قریب الوقوع اغلب آنقدر واقعی به نظر می‌رسد که قربانی را فریب می‌دهد تا پاسخ دهد. مجرمان اینترنتی آموخته اند که ایمیل‌های فیشینگ که باعث وحشت یا ترس می‌شوند، منجر به کلیک قربانی برای اطلاعات بیشتر می‌شود. به عنوان مثال، ایمیلی که ادعا می‌کند از طرف یک شرکت حقوقی درباره حضور در دادگاه با "اعلامیه دادگاه" پیوست شده است. یا ایمیلی که ادعا می‌کند از سازمان امور مالیاتی است توضیح می‌دهد که قربانی بدهکار مالیات است یا در حال بازرسی است، که این اطلاعات همراه با سند جزئیات است. قربانیانی که طعمه روانشناسی حمله فیشینگ می‌شوند و روی این پیوندهای مخرب کلیک می‌کنند یا این پرونده‌ها را بارگیری می‌کنند، اغلب در سیستم عامل‌های خود بارگیری و نصب می‌شوند.

استفاده از کلمه "عجله کن، فوری است!"

مدت هاست که بازاریابان ایمیل می‌دانند که ایجاد احساس فوریت یکی از بهترین راه‌ها برای سوق دادن کاربران به عمل است. کلماتی مانند "اکنون اقدام کن" یا "پیشنهاد امروز پایان می‌یابد" یک واکنش روانشناختی به نام FOMO ایجاد می‌کنند: ترس از دست دادن. هکرها نیز با درک این نکته که پیام‌های فوری باعث می‌شود قربانیان ابتدا اقدام کنند و بعداً فکر کنند، روی موج اضطراری پرش کردند. به عنوان مثال، هکرها از حمله مصالحه با ایمیل تجاری (BEC) استفاده می‌کنند که در آن مهاجم به یک حساب ایمیل شرکت حمله می‌کند یا خود را هک می‌کند و "یک مرجع ادراکی" مانند یک ناظر را جعل می‌کند تا قربانیان را سریع وارد عمل کند. "رئیس" ممکن است با ارسال پیام کوتاه درخواست پر کردن فرم یا پرداخت سریع را انجام دهد؛ و چه کسی می‌خواهد رئیس را با تأخیر دیوانه کند؟

پول را به من نشان بده

طرح‌های مربوط به پول مورد علاقه هکرها است، زیرا آن‌ها می‌دانند که اکثر مردم ذاتاً "حریص" هستند. متوسل شدن به تمایل قربانی برای داشتن ثروت یا قدرت قلاب اثبات شده در زمینه دستکاری روانی است. علاوه بر این، در زمان‌هایی مانند اکنون، که اخراج‌های مربوط به COVID معمول است، ممکن است قربانیان به دلیل ناامیدی یا اضطراب، روی چیزی کلیک کنند. به عنوان مثال ایمیلی از سازمان امور مالیاتی به قربانیان می‌گوید که چک‌های استرداد شده مدت‌ها در انتظار آن‌هاست و آن‌ها را به باز کردن ضمیمه دستورالعمل‌های دریافت پولشان راهنمایی می‌کند. مثال دیگر ارسال ایمیل جعلی از بانک جهت هشدار به شرکت در مورد مشکلی یا اطلاع دادن از پرداخت سود با هدف فریب آنها برای وارد کردن شناسه بانکی و رمز عبور است.

توجه کنید، جزئیات را از دست می‌دهید

هکرها با ایمیل‌های حمله مهندسی اجتماعی که شامل آرم‌هایی با ظاهر مشابه یا سایر عناصر طراحی شده برای شباهت زیاد به یک تجارت قانونی است، قربانیان را فریب می‌دهند. این ایمیل‌ها به منظور جلب توجه قربانیان در جای دیگر است، بنابراین آن‌ها جزئیات کوچکی را که باعث فریبکاری می‌شود، انتخاب نمی‌کنند. به عنوان مثال، ایمیل‌های جعلی تأیید حمل و نقل FedEX یا UPS که تشخیص آن‌ها غیر از واقعیت دشوار است. یا یک ایمیل جعلی با رمز عبور Dropbox جعلی تنظیم مجدد کرده است که باعث می‌شود کاربران بی گناه با کلیک روی پیوند "رمز ورود خود را به روز کنند". طبق گزارش Wombat’s State of the Phish email ، مثرترین ایمیل فیشینگ برای بازنشانی گذرواژه، ایمیلی است که به نظر می‌رسد از بخش فناوری اطلاعات خود شما باشد.

ایجاد اتصال شخصی

بهترین راه برای متقاعد کردن یک قربانی برای کنار گذاشتن مراقبت، ایجاد احساس اعتماد است. هکرها ممکن است سعی کنند روابط شخصی خود را با ایجاد پروفایل‌های جعلی در شبکه‌های اجتماعی و اتصال به مرور، با هدفی خاص ایجاد کنند. آن‌ها ممکن است با ارسال پست‌های شغلی جعلی از طریق LinkedIn یا ارسال لینک‌های نامناسب از طریق پیام رسانی فیسبوک، یک قربانی را به دام خود بیندازند. یا ممکن است با ربودن یک مکالمه مشروع بین دو طرف مورد اعتماد، از میانبر استفاده کنند. به گفته ZDNet، مکالمه هنگامی رخ می‌دهد که هکرها به موضوع‌های ایمیل بین دو نفر نفوذ می‌کنند، محتوای مخرب را ارسال می‌کنند در حالی که به نظر می‌رسد شخصی که قربانی با او فقط صحبت می‌کرده شخصی است که پیام را به عقب و جلو می‌فرستد.

آیا می‌توان به محافظت کامل در برابر پرونده‌های تسلیحاتی ارسال شده از طریق حملات فیشینگ دست یافت؟

دنیایی را تصور کنید که کارمندان می‌توانند بدون اینکه دوباره فکر کنند، روی هر پیوست ایمیلی که به آن برخورد می‌کنند کلیک کرده و بارگیری کنند. خوب، با استفاده از Votiro’s Secure File Gateway، محافظت کامل در برابر پرونده‌های مخرب صرف نظر از منبع فایل امکان پذیر است. برخلاف راه حل‌های امنیتی مبتنی بر ردیابی که عناصر مشکوک را اسکن می‌کند و برخی از پرونده‌های مخرب را مسدود می‌کند، فناوری انقلابی مثبت Votiro تنها عناصر ایمن هر پرونده را جدا کرده که برای کاربر اطمینان حاصل شود که صد درصد از فایلی که وارد سازمان می‌شود ایمن بوده و شامل پیوست‌های ایمیل و ایمیل خود پرونده‌ها است.

منبع: باشگاه خبرنگاران جوان