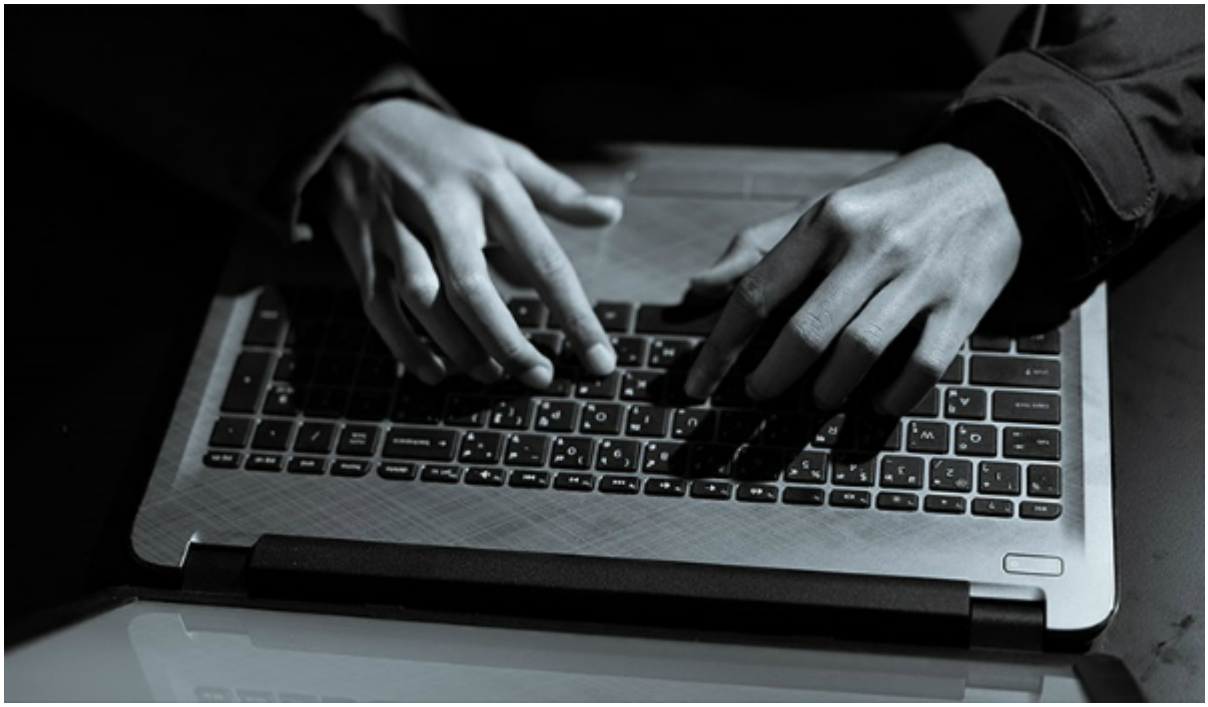
احراز هویت دو مرحله‌ی گوگل و یاهو در مقابل حملات فیشینگ دوام نیاوردند - دیجیاتو

مانی میرجوادی | جمعه، ۳۰ آذر ۱۳۹۷

طبق گزارشات موج تازه‌ای از حملات سایبری علیه اکانت‌های گوگل و یاهو در جریان است که حتی می‌تواند لایه‌ی دوم امنیت را پشت سر بگذارد. لایه‌ی دوم امنیت مربوط به ورود دو مرحله‌ای به حساب کاربری یا two-factor authentication می‌شود که حملات یاد شده می‌توانند علاوه بر گذر از این لایه، اطلاعات شخصی کاربران را سرقت کنند.

در آخرین گزارشات، حملات جدید به روش فیشینگ (تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری و رمز عبور از طریق جعل یک وب سایت و ...) صورت گرفته و حتی از لایه‌ی دوم امنیتی نیز عبور کرده است.

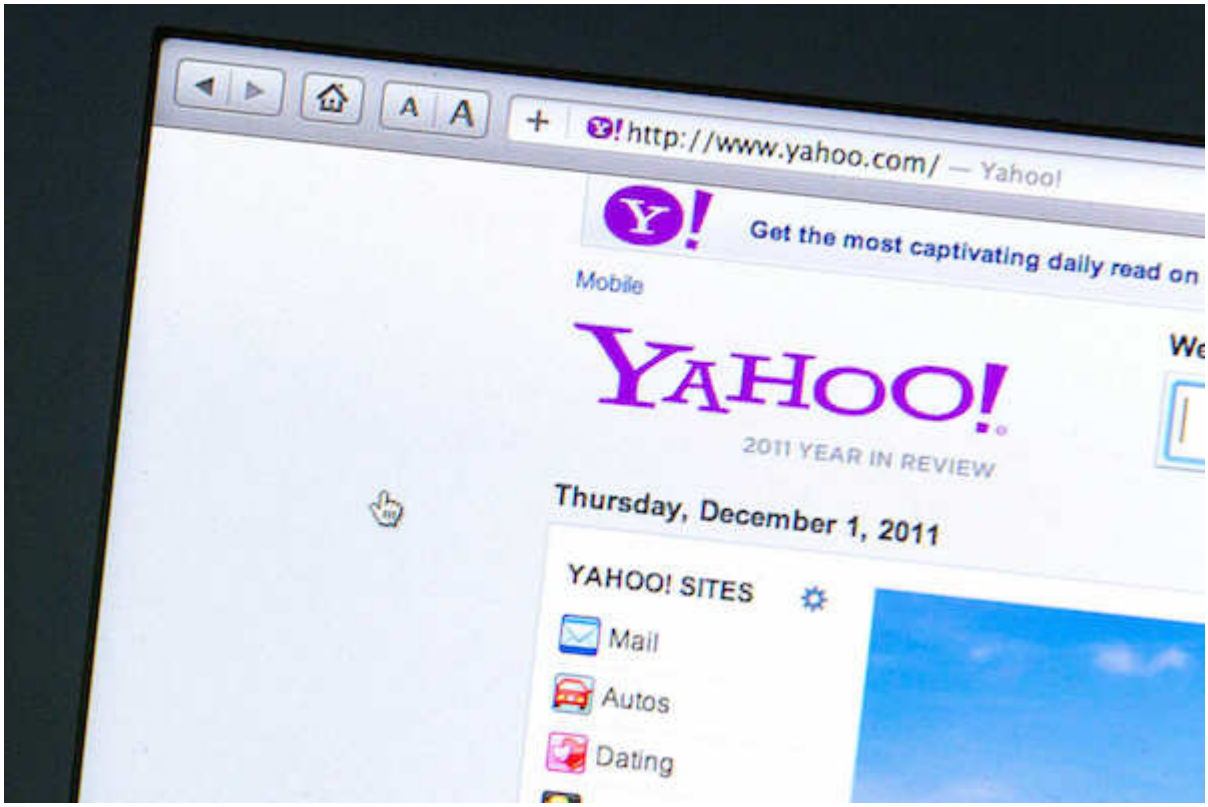
در این حملات، هکرها با ارسال پیام‌هایی با عنوان «هشدار امنیتی» افراد را به دامنه‌هایی دروغین می‌فرستادند و از آن‌ها درخواست می‌کردند تا نسبت به تغییر رمز عبور خود در حساب‌های یاهو و گوگل اقدام کنند. البته موضوعی که این حملات را متفاوت می‌کند مورد هدف قرار گرفتن لایه‌ی دوم امنیت در ورود دو مرحله‌ای به این وبسایت‌هاست.



سایت جعلی طوری طراحی شده که از افراد درخواست می‌کند تا کد مرحله‌ی دوم دریافتی از طریق پیام کوتاه را نیز وارد کنند. با وارد کردن این کد، مهاجمین کد را دریافت کرده و می‌توانند به راحتی وارد حساب کاربری افراد شوند.

از آنجایی که تمام پروسه به صورت خودکار و با استفاده از کامپیوتر شکل می‌گیرد، پیش از انقضای کد برای ورود دو مرحله‌ای مهاجمین می‌توانند وارد وبسایت شوند. این حملات به اکانت‌های گوگل هم به شکل مشابهی انجام می‌شود.

اما موج دیگر حملات، سرویس‌های ایمیل دیگری را مورد حمله قرار داد که مدعی امنیت بیشتر و قابل توجه‌تری هستند. وبسایت‌هایی مثل توتانوتا و پروتون میل.



مهاجمین برای فریب دادن قربانی‌ها سعی کردند تا وبسایت‌هایی کاملا مشابه با سرویس‌های ارائه دهنده‌ی ایمیل ایجاد کنند. برای این کار مهاجمین موفق شدند دامنه‌ی tutanota.org را ثبت نمایند -در حالی که سرویس دهنده‌ی اصلی در آدرس tutanota.com قرار دارد- و وبسایتی دقیقا مشابه با وبسایت اصلی ایجاد کنند. سپس با کشاندن قربانیان به این وبسایت‌های تقلبی اطلاعات شخصی آن‌ها را به سرقت می‌بردند.

این وبسایت‌ها همچنین از رمزگذاری در تبادل داده‌ها استفاده می‌کنند. موضوعی که باعث می‌شود قفل کنار لینک در وبسایت‌ها به رنگ سبز درآید و اطمینان کاربر را جلب کند.

مهاجمین برای حمله به کاربران ایمیل‌های پروتون میل نیز با ساخت دامنه‌ی protonemail.ch افراد را فریب دادند (این دامنه یک e اضافه دارد). در حال حاضر دامنه‌ی یاد شده بسته شده است.

سازمان عفو بین الملل بر این عقیده است که مرکز اصلی این حملات کشورهای حاشیه‌ی خلیج فارس هستند و بیشتر چهره‌های سیاسی، ژورنالیست‌ها و فعالین حقوق بشر مورد هدف قرار گرفته‌اند.

دیجیاتو