سه شنبه 23 اسفند 1390 - 07:53

فیشینگ تهدیدي جدي براي کاربران

آیا تا به‌حال درباره عبارت فیشینگ (Phishing) شنیده‌اید؟ حتما بسیاری از شما با مفهوم این عبارت آشنایی دارید.

جام جم آنلاین: آیا تا به‌حال درباره عبارت فیشینگ (Phishing) شنیده‌اید؟ حتما بسیاری از شما با مفهوم این عبارت آشنایی دارید. ولی واقعا فیشینگ چیست؟ این عبارت ممکن است برای برخی کاربران اینترنت، عبارت جدیدي نباشد ولی نباید فراموش کنیم که میلیاردها کاربر اینترنت وجود دارد و از این میان، میلیون‌ها نفر در دام کلاهبرداری فیشینگ افتاده‌اند.

فیشینگ چیست؟

فیشینگ یک تکنیک مهندسی اجتماعی است که به‌وسیله یک هکر یا حمله‌کننده برای دزدیدن اطلاعات حساس مانند نام کاربری، رمز عبور و رمز کارت‌های اعتباری استفاده می‌شود (در این حالت حمله‌کننده وانمود می‌کند یک شخص یا یک سازمان مورد اعتماد است).

امروزه اغلب کاربران با دنیای آنلاین عجین شده‌اند، در حالی که شاید از خطرات معمول این دنیا بی‌اطلاع باشند.

یک هکر یا یک حمله‌کننده می‌تواند هرکسی را براحتی در دام کلاهبرداری فیشینگ خود بیندازد البته تمام این مساله به کاربر بستگی دارد که برای شناسایی و ممانعت به عمل آوردن فیشینگ، هوشمندانه عمل خواهد کرد یا خیر. هرچند فیشینگ یک بدافزار نیست، ولی به این معنی نیست که خطر کمی برای کاربر دارد. هر کاربر اینترنت باید از خطرات این گونه کلاهبرداري آگاه باشد.

انواع مختلف حمله فیشینگ

فیشینگ فریبنده: در این نوع از روش‌های فیشینگ، یک هکر از ایمیلي فریبنده برای کلاهبرداری از کاربر استفاده می‌کند. او حجم زیادی از این ایمیل‌های به ظاهر جذاب که کاربر را مجاب می‌کند روی لینکی که در ایمیل قرار داده شده است کلیک کند، ارسال می‌کند سپس هکر از کاربر می‌خواهد اطلاعات حساب خود را در جایی وارد کند و بعد از آن تنها کاری که هکر نیاز است انجام دهد، جمع‌آوری اطلاعاتی است که کاربر در اختیار او قرار داده است.

جعل وب‌سایت‌ها: امروزه این روش، معمول‌ترین راه برای کلاهبرداری از کاربران اینترنتی است. در این روش، هکر، مسیر کاربر را به یک URL (وب‌سایت) جعلی که بسیار شبیه وب‌سایت اصلی است، تغییر می‌دهد. هکر همچنین می‌تواند از آسیب‌پذیری وب‌سایت سوءاستفاده کند و کاربر را به دام بیندازد. آنها می‌توانند یک جاوااسکریپت را به‌منظور تغییر نوار آدرس به وب‌سایت تزریق کنند یا از نقاط ضعف XSS (اسکریپت‌نویسی بین سایتی) نهایت استفاده را ببرند.

فیشینگ تلفنی: در این نوع از فیشینگ، یک هکر خود را به‌عنوان شخصي مورد اعتماد و نماینده موسسه یا شرکتي معتبر معرفی کرده و اطلاعات مهم را از طریق تلفن از شنونده دریافت می‌کند. این روش نه به وب‌سایت نیاز دارد و نه به هیچ‌گونه ایمیل.

قاپیدن تب: این روش جدیدترین روش فیشینگ است. قاپیدن تب، روشی است که وقتي یک کاربر چند تب باز دارد، به‌طور خودکار (و البته کاملا آرام) آن کاربر را به سایت یک حمله‌کننده هدایت می‌کند.

چگونه می‌توانیم یک کلاهبرداری فیشینگ را شناسایی کنیم؟

اول، دریافت ایمیل از بانک‌تان یا هر موسسه و سازمانی با این مضمون که «به‌علت فعالیت‌های غیرمجاز، حساب شما در حال بسته شدن است، جهت جلوگیری از تعلیق، حساب خود را بازبینی و تایید کنید».

اگر چنین ایمیلی دریافت کردید، نباید به آن اهمیت دهید. همچنین ممکن است ایمیلی دریافت کنید که در آن نوشته شده باشد «شما در قرعه‌کشی برنده هزار دلار شده‌اید و برای واریز این پول، اطلاعات حساب خود را وارد کنید» که نباید به‌هیچ وجه آن را باور کنید. در مقابل این‌گونه ایمیل‌ها، هوشمندانه عمل کنید.

نکته دوم این‌که ایمیل‌های فیشینگ یک شخص خاص را مورد خطاب قرار نمی‌دهد و در اغلب موارد برای حجم زیادی از کاربران

ارسال می‌شود.

از آنجا که کاربران هدف به‌صورت تصادفی انتخاب می‌شوند، احتمالا در ابتدای ایمیل‌ها عباراتی نظیر «مشترک گرامی« ،raquo;کاربر گرامی سایت PayPal» و غیره را مشاهده کنید.

آنها معمولا اسم شما را خطاب قرار نمی‌دهند بنابراین اگر چیزی شبیه اینها دیدید به این فکر کنید که ممکن است در دام این شیوه از کلاهبرداري اینترنتي افتاده‌اید.

و آخرین نکته درباره URL فیشینگ است. این امکان وجود دارد به وب‌سایتی هدایت شوید که کاملا شبیه سایت اصلی باشد، ولی باید بدانید ممکن است به سایت فیشینگ رفته باشید.

همواره به URL نگاه کنید تا متوجه شوید آیا در وب‌سایت اصلی هستید یا یک وب‌سایت فیشینگ (وب‌سایت تقلبی).

چگونه از فیشینگ اجتناب کنیم؟

هیچ‌گاه به ایمیل‌هاي مشکوک که از شما اطلاعات شخصی‌تان را می‌خواهد پاسخ ندهید. همواره قبل از پاسخ دادن یا کلیك روي لینك معرفي شده، ابتدا به منبع آن توجه کنید.

از کلیک کردن روی ابرلینک‌ها پرهیز کنید؛ هنگامی که یک ایمیل را بررسی می‌کنید، روی ابرلینک‌هایی که در آن وجود دارد کلیک نکنید، بویژه اگر از یک منبع نامطمئن آن را دریافت کرده‌اید.

شما هرگز متوجه نخواهید شد به کجا فرستاده می‌شوید یا ممکن است با این کار یک کد مخرب را فعال کنید.

برخی ابرلینک‌ها ممکن است شما را به وب‌سایت‌های جعلی که اطلاعات ورود شما را درخواست می‌کنند، هدایت کنند.

همیشه سعی کنید اطلاعات‌تان را در مقابل آخرین تهدیدات امنیتی به‌روز نگه دارید.

بیاموزید چگونه آنها را شناسایی و از آنها دوری کنید. تنها کمی جستجو و تحقیق در اینترنت می‌تواند شما را در برابر خسارت‌های بزرگ حفظ کند.

محمدحسین کردونی - منبع: itechcrazy