SANS SECURITY AWARENESS

OUCH!

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

جلوگیری از حملات فیشینگ

مقدمه

یکی از اولین راه هایی که برای تبادل ارتباطات وجود دارد، استفاده از ایمیل و سرویس های پیام رسان (نظیر اسکایت، توییتر و تلگرام) است. امروزه نه تنها از این تکنولوژی ها برای کارهای روزانه استفاده میشود بلکه راهی است برای در ارتباط بودن با دوستان و خانواده. از آنجاییکه افراد زیادی در سرتاسر دنیا به این تکنولوژی ها وابسته هستند، استفاده از آن نیز یکی از اولین روش های حملات سایبری توسط هکرها شده است که به این روش حمله، فیشینگ گفته میشود. در این شماره به شما خواهیم گفت که فیشینگ چیست و چگونه میتوان این گونه حملات را چه در محل کار و چه در منزل، مشاهده و دفع کرد.

فیشینگ چیست

فیشینگ نوعی حمله است که در آن با استفاده از سرویس های پیام رسان و ایمیل سعی میکنند شما را فریب بدهند تا عملی را انجام بدهید که نباید، این کارها میتوانند کلیک کردن روی لینک آلوده، به اشتراک گذاری رمزعبور و یا باز کردن یک فایل آلوده در ضمیمه ایمیل باشد. هکرها به شدت کار میکنند تا این پیام ها به حدی متقاعد کننده باشند تا باعث فعال شدن احساساتی نظیر کنجکاوی و نیاز در شما بشوند. آنها میتوانند پیغام فیشینگ را به گونه ای درست کنند که به نظر برسد از طرف کسی یا جایی که میشناسید، مثلا توسط یک دوست و یا یک شرکتی که با آنها در ارتباط هستید، ارسال شده است. یا شاید لوگوی بانک شما را به همراه ایمیلی که قانونی به نظر میرسد برای شما ارسال کنند. هکر ها این گونه پیغام ها را برای میلیونها نفر ارسال میکنند. آنها نمیدانند چه کسی در این دام خواهند افتاد، چیزی که میدانند این است که هرچه بیشتر ارسال کنند قربانی بیشتری خواهند داشت.

محافظت از خود

در اکثر موارد، باز کردن و خواندن یک ایمیل و یا یک پیغام خوب است. برای اینکه حمله فیشینگ اتفاق بیافتد، هکر ها میبایست با فریب دادن شما از شما بخواهند کاری را انجام بدهید. خوشبختانه راه حل هایی وجود دارد که بتوان تشخیص داد آیا یک پیغام حمله است یا خیر، در ذیل معمول ترین این روش ها را بررسی میکنیم:

- القای حس فوریت، درخواست «اقدام فوری» قبل از اینکه اتفاق بدی بیافتد، نظیر تهدید به بستن حساب شما و یا زندانی کردن فرد. هکر ها از شما میخواهند با عجله عملی را انجام بدهید که موجب بروز اشتباه شود.
- اعمال فشار به شما برای نادیده گرفتن و یا دور زدن سیاست ها و یا روال ها در محل کار
- ایجاد حس کنجکاوی و یا حسی که برای درست بودن بیش از حد خوب به نظر برسد (خیر، شما برنده قرعه کشی نشدید).

- احوال پرسی عمومی نظیر «مشتری عزیز». بیشتر دوستان و شرکتها در زمان ارسال پیام نام شما را میدانند.
- درخواست اطلاعات با حساسیت بسیار بالا، نظیر شماره کارت اعتباری یا رمزعبور یا هراطلاعاتی که تنها مراکز قانونی باید بدانند.
- پیغامی که به نظر میرسد از یک سازمان رسمی ارسال شده است درحالیکه حاوی گرامر ضعیف یا غلط های املایی یا استفاده از آدرس ایمیل غیر رسمی نظیر @gmail.com است
- پیغام از یک آدرس ایمیل رسمی (مثلا ایمیل رییس شما) آمده است درحالیکه در زمان ارسال پاسخ (Reply-To) جواب آن به آدرس شخصی فرد دیگری ارسال میشود.
- پیامی را از فردی که میشناسید دریافت میکنید، اما ادبیات و نوع نوشتار شبیه ادبیات او نیست.اگر به این امر مشکوک هستید، با فرستنده آن تماس بگیرید و مطمئن شوید خودش آن را ارسال کرده است. برای هکر ها ایجاد یک پیام که مشابه پیامی باشد که از طرف یک دوست و یا همکار دریافت میکنید کار ساده ای است.

در نهایت بهترین کار استفاده از عقل سلیم است. اگر یک ایمیل و یا یک پیام به نظر عجیب و غریب میرسد، مشکوک است و یا بیش از حد خوب به نظر میرسد، ممکن است یک حمله از نوع فیشینگ باشد.

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

سردبیر مهمان

تونیا دادلی(**Tunia Dudley**) از سال 2011 در حال توسعه و اجرای برنامه های آگاهی رسانی امنیتی میباشد، این آگاهی رسانی شامل تهیه یک برنامه آموزش فیشینگ است که برنده جوایزی شده است.برای برقراری ارتباط با ایشان از این لینک استفاده کنید www.linkedin.com/in/toniadudley.

منابع

مهندسی اجتماعی:	https://www.sans.org/u/Cb1
کمک به دیگران امن کردن آنها:	https://www.sans.org/u/Cb6
باید ها و نباید های ایمیل:	https://www.sans.org/u/Cbg
فریب مدیر:	https://www.sans.org/u/Cbl
آرشیو و ترجمه های ماهنامه وای:	https://www.sans.org/u/Cbq

مجوز