فیشینگ و راه‌های مقابله (حملات مهندسی اجتماعی و کلاهبرداری)

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶ رقمی عابر بانک، رمز دوم و CVV2 را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می برند. شبکه های اجتماعی، سایت های حراجی و درگاه های پرداخت آنلاین نمونه ای از ابزار های الکترونیکی ارتباطات می باشند.

کلاهبرداری فیشینگ از طریق ایمیل ها و پیامها صورت می پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در وب سایت های جعلی که در ظاهر کاملا شبیه وب سایت های سالم و قانونی می باشد وارد می نمایند. حقه ی فیشینگ یکی از تکنیک های مهندسی اجتماعی برای فریب کاربران می باشد که علی‌القاعده از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می کنند. برای اولین بار حقه ی فیشینگ در ۱۹۸۷ تعریف شد و اولین باری که واژه فیشینگ برای نام گذاری این واژه استفاده گردید، سال ۱۹۹۶ بود.

انواع مختلف فیشینگ کدام است؟

فیشینگ انواع مختلفی دارد که به روش های مختلف تلاش می‌کنند به اطلاعات بانکی شما از طریق روش های متنوع مهندسی اجتماعی (Social Engineering) که در حوزه فیشینگ مانند ایمیل، تماس تلفنی، صفحات جعلی پرداخت، پیامک، انواع مدل های ربات های تلگرام و انواع روش های جدیدی که انتظار آن نمی رود، دست یابد. برخی از معروف‌ترین روش‌های فیشینگ عبارت اند از:

فیشینگ با ایمیل‌های فریبنده

در این روش از حمله‌های فیشینگ، شخص کلاهبردار با ارسال ایمیل‌های فریبنده به قربانیانش می‌کوشد با بیان دلایل مجاب کننده مخاطبان را به وارد کردن اطلاعات بانکی خود وادار کند.

ممکن است ایمیل به ظاهر از طرف بانک شما، یک شرکت معتبر یا حتی بانک مرکزی ارسال شود و از شما درخواست کند ظرف زمان معینی اطلاعات بانکی خود را ارسال کنید. متاسفانه بارها افرادی فریب این حملات فیشینگ را خورده‌اند.

نکته: سیستم مالی و بانکی هیچگاه از طریق ایمیل از شما درخواست نمی‌کند اطلاعات بانکی‌تان را برای آن‌ها ارسال کنید، شما حتی مجاز به اعلام رمز بانکی خود به کارکنان بانک هم نیستید.

فیشینگ تلفنی

هکرها در این روش از طریق تلفن با طعمه های خود ارتباط برقرار می‌کنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما می‌شناسید معرفی می‌کنند از شما می خواهند جهت دریافت جایزه خود اطلاعات بانکی خود را در اختیار ایشان قرار دهید. یا در روشی دیگر، با ارسال پیامک به شماره همراه شما، اعلام می کنند که حساب بانکی شما دچار مشکل شده است و شما را به زنگ زدن به شماره تماسی جعلی (سرویس تلفن اینترنتی) سوق می دهند و در ادامه از شما شماره حساب و رمز کارت و یا حتی رمز دوم را می خواهند.

نکته: برای واریز هر گونه وجه به حساب شما اعم از جایزه، پاداش و مزایا نیازی به اعلام رمز بانکی شما نخواهد بود. برای مقابله با هکرها و حملات فیشینگ این نکته را فراموش نکنید.

طراحی صفحه‌ای نظیر درگاه پرداخت بانک

شخص هکر در این روش صفحه‌ای مشابه درگاه پرداخت آنلاین بانک‌ها طراحی می‌کند و با قرار دادن این صفحه جعلی در فروشگاه‌های صوری و با ارائه پیشنهادهای وسوسه کننده خرید سعی می‌کند شما را وادار کند وارد صفحه پرداخت جعلی که طراحی کرده بشوید و وجه انتقال دهید.

به محض ورود به این صفحه جعلی و ارائه اطلاعات بانکی اطلاعات شما به صورت خودکار برای هکر ارسال می‌شود و او قادر خواهد بود حساب شما را خالی کند.

امن‌ترین درگاه پرداخت، درگاه پرداخت بانک مرکزی به آدرس https://xxx.shaparak.ir است و در کنار آن حتما باید نام یکی از pspها (شرکت های پرداخت الکترونیک) مطرح درج شده باشد .

نکته: بهترین روش مقابله با این نوع از حمله‌های فیشینگ دقت به URL درگاه پرداخت است.

درگاه‌های پرداخت بانک‌ها از کدهای امنیتی باضریب اطمینان بالا استفاده می‌کنند و اغلب در آدرس سایت عبارت https:// قابل مشاهده خواهد بود.

فیشینگ با دستگاه‌های POS و ATM تقلبی

برخی کلاهبرداران با استفاده از POS و ATM تقلبی کارت‌های بانکی طعمه های خود را کپی کرده و به بهانه فروش محصول و کالا رمز عبور آن‌ها را می‌پرسند و سپس به راحتی حساب بانکی افراد را خالی می‌کنند.

نکته:

بهتر است هیچ گاه رمز عبور خود را در اختیار فروشندگان قرار ندهید. با پیشرفت تکنولوژی شیوه‌های پرداخت متنوعی در اختیار شما قرار گرفته که با کمک آن می‌توانید استفاده از POS و ATM را به میزان قابل توجهی کاهش دهید. دریافت دستگاه های POS اختصاصی توسط شرکت‌ها و سازمان‌ها هم می‌تواند به جلب اعتماد بیشتر مشتریان کمک کند.

ربات تلگرام و فیشینگ

ربات‌های تلگرام این روزها به بسیاری از کارهای ما سرعت بخشیده‌اند، شرکت‌های معتبر هم در این خصوص خدمات خوبی را ارائه می‌دهند که گزارش گیری انتقال وجوه را ساده تر کرده است. اما به هر حال تلگرام بستر مناسبی برای انتقال وجه نیست و دیده شده به بهانه انتقال وجه و یا حتی دریافت خدمات و یا خرید محصولی و یا حتی با نوشتن پست های وسوسه برانگیز و تحریک افراد برای عضو شدن در کانال و یا گروه هایی، اطلاعات بانکی حساب و یا کارت بانکی شخص را سرقت می کردند.

روش های کاربردی در مقابله با فیشینگ

با توجه به مواردی که مطرح شد، راه هایی در مورد مقابله و جلوگیری از گیر افتادن در دام فیشر ها وجود دارد که از میان آنها می توان به موارد زیر اشاره داشت:

- یکی از بهترین راه ها برای دستیابی به صفحات وب، نوشتن آدرس آن به طور مستقیم در مرورگر است. یک ایمیل یا پیامک کلاهبرداری، این امکان را دارد که ادعا داشتن اعتبار لازم را داشته و از بانک ، شرکت و یا مؤسسه معتبری ارسال شده باشد. هنگامی که شما روی لینکی که برای شما ارسال شده کلیک کنید با سایتی مشابه با سایت واقعی و به ظاهر معتبر مواجه می‌شوید که با پر کردن اطلاعات خود در آن، امکان به سرقت رفتن اطلاعاتتان را فراهم می کنید. برای جلوگیری از این اتفاق همیشه دنبال منابع معتبر بروید و در صورت دریافت ایمیلی با مقدمه های وسوسه بر انگیز، به جای بازگشایی بلافاصله آن به آدرس اصلی سایت مطرح شده را در مرورگر خود وارد کنید. سعی کنید امنیت اکانت ایمیل خود را افزایش دهید.
- استفاده از رمز یکبار مصرف را جدی بگیرید؛ این **رمز یکبار مصرف** ها با اعتباری که در زمان کم دارند، باعث جلوگیری از به سرقت رفتن اطلاعات شما می شود.
- فرستنده یا فرستاده‌ی غیر معمول؛ اگر پیامک یا ایمیلی از شخص ناشناسی که دارای لینکی که برای دریافت جایزه یا قرعه کشی بود و حتی اگر این پیام از طرف شخصی بود که او را می شناختید، به هیچ وجه بر روی آن لینک کلیک نکنید.
- هدایت به دامنه‌ی فیشینگ به جای سایت واقعی؛ همانطور که در قسمت های بالا هم گفته شد، همیشه قبل از انجام تراکنش آدرس URL درگاه پرداخت را حتما بررسی کنید.