فیشینگ چیست؟

فیشینگ یا سرقت آنلاین، نوعی حمله مهندسی اجتماعی است که عموماً از طریق ایمیل و با هدف سرقت اطلاعات ورود به سیستم و سایر اطلاعات حساس مانند نام کاربری، گذرواژه یا رمز عبور، اطلاعات حساب بانکی، شماره ۱۶ رقمی عابر بانک، رمز دوم و CVV2 و مانند آن‌ها از طریق جعل یک وبگاه، آدرس ایمیل و مانند آن‌ها برای سرقت هویت افراد انجام می شود.

در حمله فیشینگ، هکرها از ارتباطات نوشتاری (به عنوان مثال ایمیل یا پیام فوری) برای سرقت اطلاعات شخص به عنوان یک منبع معتبر استفاده می کنند. در واقع هدف این است که گیرنده ایمیل فریب بخورد و با تصور اینکه پیام مورد نظر چیزی است که او می خواهد، روی لینک کلیک کرده و یا پیوست را بارگیری کند. معمولا این روند مراحل زیر را طی می کند:

- هکر به یک وب سایت معتبر دسترسی پیدا کرده یا یک دامنه جعلی ایجاد می کند.
- مهاجم پیامی را طراحی می کند که دریافت کنندگان را به کلیک بر روی لینک ارسالی به آن سایت ترغیب کرده و این پیام را به ایمیل های متعددی ارسال می کند.
- اگر شخصی روی لینک کلیک کند، یا از آن ها خواسته می شود نام کاربری و رمزعبور خود را وارد کنند و یا سایت بدافزاری را بارگیری می کند که اطاعات ذخیره شده در دستگاه یا حافظه مرورگر را جمع آوری می کند.
- مهاجم از این اعتبارها برای دزدیدن داده های حساس از شخص استفاده می کند.

اگرچه فیشینگ برای هدف قرار دادن افراد طراحی شده است اما در صورت موفقیت آمیز بودن یک حمله فیشینگ عواقب جبران ناپذیر هم افراد و هم سازمان ها را درگیر خواهد کرد.

مجرمان اینترنتی می توانند با داشتن اطلاعات کاربری وارد سیستم شده، به برنامه های شخصی و شرکتی دسترسی پیدا کنند و با تغییر رمز عبور دسترسی مالکین را به حساب ها قفل کنند. آن ها همچنین می توانند با اضافه کردن عوامل احراز هویت چندعاملی با دستگاه های خود امکان دسترسی به حساب ها را سخت تر کنند.

این موضوع به خصوص زمانی مشکل ساز می شود که مهاجم از طریق ایمیل پیام های ظاهرا قانونی را به کاربران مختلف ارسال کرده و در نهایت کل شبکه به خطر می افتد.

پس از ورود به شبکه سازمان، هکرها می توانند با استفاده از مجوزهایی که از افراد به دست آورده اند به نصب بدافزارهایی اقدام کنند که می توانند سیستم های شرکتی را خاموش کرده و یا پول و مالکیت معنوی را سرقت کنند.

به دلیل سطح کنترلی که مدیران در سازمان خود دارند حمله والینگ می تواند تاثیر شدیدی بر شرکت بگذارد. این حملات می تواند خسارت زیادی به سازمان ها وارد کند.

علاوه بر خسارت مالی و از دست رفتن سرمایه سازمان در مواردی داده های مشتری به خطر افتاده و اعتبار سازمانی آسیب دیده است.

اطلاعاتی که سایت‌های فیشینگ ممکن است از کاربران بخواهند

- نام کاربری و رمز عبور
- شماره تلفن ها
- شماره های مربوط به حساب های بانکی
- کدهای خصوصی مربوط به هر شخص
- شماره های مربوط به کارت های اعتباری
- سال روز تولد
- اطلاعات مربوط به هویت
- پرسش سوال هایی مانند آنچه دوست دارید؟
- درخواست اطلاعات خانوادگی

راه های پی بردن به صفحات فیشینگ

- یکی از راه های اصلی پی بردن به جعلی بودن درگاه پرداخت این است که دامنه شاپرک فقط ir . است. بنابراین در صورتی که با دامنه های com. و org. و یا سایر دامنه ها مواجه شدید، قطعا درگاه پرداخت جعلی است.
- بررسی اینکه آیا دامنه اصلی دقیقا برابر shaparak.ir است، جهت اطمینان حاصل کردن از اصلی بودن درگاه پرداخت کافی است.
- رمز دوم یکبار مصرف (رمز پویا) کارت بانکی خود را فعال کنید تا در صورتی که اطلاعات کارت بانکی شما به سرقت رفت، مهاجمان نتوانند مبلغ زیادی را از حساب شما برداشت کنند.

روش های شکایت از کلاهبرداری اینترنتی

برای هر یک از ما که درگیر چنین اتفاقی شده‌ایم، چند روش پیگیری وجود دارد. بعد از ثبت نام در سامانه سراسری ابلاغ قوه قضاییه با نام اختصاری ثنا به یکی از دو روش می‌توان شکایت خود را مطرح کنیم. مراجعه به یکی از دفاتر خدمات الکترونیک قضایی و ثبت شکایت کیفری و یا ثبت شکایت از طریق وکیل متخصص جرایم رایانه‌ای و مراجعه مستقیم به دادسرای جرایم رایانه‌ای و ثبت شکایت جهت ارجاع به پلیس فتا از جمله این اقدامات است.

سخن پایانی

در برخی موارد کاربران به دلیل سهولت کار، اقدام به جستجوی اینترنت بانک یا موبایل بانک مورد نظر در موتورهای جستجوگر اینترنتی می‌کنند که با ورود به سایت‌های جعلی، اطلاعات حساب کاربری شامل؛ نام کاربری، رمز ورود و سایر اطلاعات بانکی آن‌ها توسط فیشرها به سرقت می‌رود. باید آدرس اینترنت بانک و یا موبایل بانک را از سایت رسمی بانک مربوطه دریافت کنند و همچنین از کلیک کردن بر روی لینک‌های ناشناس ارائه شده در شبکه‌های اجتماعی و سایت‌های نامعتبر خودداری نمایید.

یادآوری

در هفته چهارم در مورد حملات فیشینگ یا سرقت آنلاین مطالبی را برای همکاران عزیز ارائه نمودیم ، مطلب مورد بحث فوق در رابطه با پاسخ به سئوالات کاربران و بحث تکمیلی این موضوع در این هفته بود .