فیشینگ و راه‌های مقابله با آن

آقای بهنام متقیان
حوزه معاونت بانکداری الکترونیکی

«**فیشینگ**» (Phishing)، به نوعی کلاه برداری برای به‌دست آوردن اطلاعات کارت یا حساب بانکی از طریق تماس‌تلفنی، جعل یک تارگاه، نشانی پست‌الکترونیکی و ... گفته می‌شود.

فیشینگ، راهی است که کلاه برداران، اطلاعاتی نظیر: نام کاربری، رمز عبور، شماره کارت بانکی، رمز دوّم و CVV2 را از طریق ابزارهای الکترونیکی و ارتباطی به سرقت می‌برند.

شبکه‌های اجتماعی و تارگاه‌های پرداخت آنلاین، از جمله اهداف حملات فیشینگ هستند. علاوه بر آن، تماس‌های تلفنی کلاه برداران که خود را از مسؤولان بانک معرفی می‌کنند و پست‌های‌الکترونیکی که با این هدف، ارسال می‌شوند و حاوی پیوندی به یک تارگاه هستند، از جمله ترفندهای فیشینگ به‌شمارمی‌رود.

نحوه کار فیشینگ

فیشینگ در عمل، به‌صورت ایجاد کپی دقیق رابط گرافیکی یک تارگاه معتبر مانند: بانک‌ها انجام می‌شود. ابتدا کاربر از طریق پست‌الکترونیکی و یا آگهی‌های تبلیغاتی تارگاه‌های دیگر به این صفحه جعلی راهنمایی می‌شود. سپس از کاربر درخواست می‌شود تا اطلاعات کارت یا حساب خود را وارد نماید و به این صورت، کلاه برداران به اطلاعات اصلی حساب یا کارت افراد دسترسی پیدا می‌کنند.

روش‌های مختلف فیشینگ

جعل و دستکاری پیوندها و نشانی‌ها

این روش یکی از شیوه‌های متداول فیشینگ است. در این روش، پیوندها و نشانی‌های غیرواقعی و جعلی سازمان‌ها و شرکت‌های معتبر، از طریق پست‌الکترونیکی به افراد ارسال می‌شود. این آدرس‌ها با نشانی‌های اصلی، تنها در یک یا دو حرف تفاوت دارند و کلاه برداران با این روش، افراد را به سمت تارگاه‌های جعلی هدایت می‌کنند.

گریز از فیلترها

کلاه برداران برای جلوگیری از شناسایی متن‌های متداول فیشینگ در پست‌های‌الکترونیکی توسط فیلترهای ضدفیشینگ، از عکس به‌جای نوشته استفاده می‌کنند.

کلاهبرداران برای جلوگیری از شناسایی متن‌های متداول فیشینگ در ایمیل‌ها توسط فیلترهای ضدفیشینگ، از عکس به‌جای نوشته استفاده می‌کنند.

جعل تارگاه

در این نوع فیشینگ، کلاه برداران با ایجاد تارگاه جعلی یک سازمان یا بانک، به‌محض وارد نمودن کلمه کاربری و رمز عبور توسط کاربر، این اطلاعات را ثبت و از آن سوءاستفاده می‌نماید.

فیشینگ تلفنی

تمامی حملات فیشینگ، نیاز به استفاده از یک تارگاه جعلی و ساختگی ندارند. این نوع حملات، شامل پیام‌هایی هم می‌شوند که ادعا می‌کنند از طرف بانک هستند و از مشتریان (استفاده‌کنندگان خدمات بانکی) می‌خواهند با توجه به مشکلی که برای حساب‌های آن‌ها به وجود آمده است، با یک شماره تماس بگیرند. به‌محض این‌که مشتری با این شماره تلفن (که متعلق به مهاجم است و یک سرویس تلفن اینترنتی است) تماس بگیرد، دستوراتی به مشتری داده می‌شود تا شماره حساب و رمز خود را وارد کند. کلاه برداران که از سرویس تلفن اینترنتی استفاده می‌کنند، گاهی اوقات از داده‌های جعلی برای Caller ID استفاده می‌نمایند تا برای مشتریان این‌گونه به نظر برسد که این تماس از طرف یک سازمان مطمئن و معتبر و یا بانک انجام می‌شود.

روش‌های مقابله با فیشینگ (برای دارندگان حساب‌های بانکی)

- اطلاعات محرمانه مربوط به حساب یا کارت بانکی خود را در اختیار دیگران قرار ندهید.
- به نشانی تارگاه و یا پست الکترونیکی دریافت شده دقت فرمایید. به‌عنوان مثال؛ در زمان ورود به حساب‌های مهم مانند: پست الکترونیکی و یا بانک، قبل از وارد کردن نام کاربری و رمز عبور، دقّت به نشانی تارگاه امری ضروری است.
- در صورت ارسال پیام یا تماس تلفنی افرادی که خود را از مسؤولان بانک معرفی می‌نمایند و اطلاعات حساب یا کارت بانکی شما را درخواست می‌نمایند، موضوع را با مرکز تماس بانک در میان بگذارید.
- رمز عبور مربوط به حساب بانکی یا پست الکترونیکی نباید کوتاه بوده یا از سوی دیگران قابل حدس باشد.
- به پست‌های الکترونیکی که در آن‌ها، از شما خواسته شده تا فرمی را پر کنید، هرگز اطمینان نکنید.
- اطلاعات حساب کاربری خود را در اختیار دیگر تارگاه‌ها قرار ندهید.
- در پرداخت آنلاین، فقط از درگاه‌های مخصوص بانک‌ها استفاده نموده و اصالت آن‌ها را بررسی نمایید.

منبع: پلیس فتا www.cyberpolice.ir