کد خبر: ۴۸۷۵۴۲
دوشنبه ۸ خرداد ۱۴۰۲ ۸:۴۱

روی این لینک کلیک نکنید!

در حالی که سودجویان از راه‌های مختلف برای کلاهبرداری و فریب کاربران استفاده می‌کنند، کلاهبرداری از طریق لینک شخصی این روزها بیش از گذشته شایع شده و به‌همین دلیل همواره توصیه می‌شود که کاربران در مواجهه با موارد مشکوک هوشیار باشند.

به گزارش سایت خبری پرسون، یکی از اقدامات کلاهبرداران این است که با راه‌اندازی سایت‌های جعلی که شبیه به سایت‌های اصلی است، به ربودن اطلاعات افراد، اغلب برای سوءاستفاده‌های مالی اقدام می‌کنند؛ در این شیوه که اصطلاحاً به فیشینگ معروف است، از طریق اطلاعات واردشده توسط کاربران در صفحات جعلی حساب‌های بانکی قربانیان خالی می‌شود. از طرفی یکی از شگردهای کلاهبرداران سایبری برای در طعمه قرار دادن مردم این است که با سوءاستفاده از احساسات شهروندان به ارسال لینک‌های حاوی بدافزار و سرقت اطلاعات شهروندان اقدام می‌کنند.

به عبارتی فیشینگ یک تهدید سایبری محسوب می‌شود و اگر بخواهیم در برابر تهدیدات سایبری ایمن باشیم، باید موارد امنیتی را رعایت کنیم. یکی از موارد امنیتی این است که هوشیار باشیم، هر ایمیلی را باز نکرده و روی هر لینکی کلیک نکنیم، آدرس سایت‌ها را دقیق چک کنیم که همان آدرس مورد نظر باشد، زمانی که یک سایت ما را به مرحله پرداخت هدایت می‌کند، دقت کنیم که مثل همان نوشته شده باشد.

بقیه موارد امنیتی هم اینگونه است که لازم بوده سیستم عامل و مرورگرمان را همیشه به‌روز کنیم، آنتی‌ویروس اصلی و معتبر داشته باشیم که ویژگی‌های امنیت اینترنتی داشته باشد، از جمله ویژگی حفاظت در برابر وب‌سایت‌ها و لینک‌های آلوده. مرورگرها معمولاً از طرف آنتی‌ویروس افزوده می‌شود و آن‌ها بخش زیادی از فیشینگ را تشخیص می‌دهند؛ هم‌چنین اگر لینک پرداخت از طریق ایمیل ارسال شد نباید از طریق آن به اینترنت بانک و ایمیل خود وارد شویم.

در این روش، کلاهبرداران سایبری از عدم آگاهی بسیاری از کاربران استفاده کرده و با شگردهای جدید سعی بر فریب کاربران و سرقت اطلاعات حساب بانکی آن داشته و در جدیدترین شیوه‌های کلاهبرداری با ارسال پیامک‌های حاوی لینک‌های جعلی در این خصوص اقدام می‌کنند.

در این شیوه جدید کلاهبرداری، کلاهبرداران در ابتدا پیامکی با مضمون داشتن پیامی جدید در این سامانه‌های الکترونیک اعلام‌شده و کاربر را برای مشاهده این پیام و پرداخت وجه به سایت جعلی بانک هدایت کرده و اطلاعات حساب بانکی آن‌ها را سرقت می‌کنند. کلاهبرداران پس از ارسال پیامک به شهروندان، به منظور واریز وجه پول دریافتی آنان را به سایت‌های جعلی و فیشینگ خود در فضای مجازی هدایت و با سرقت اطلاعات بانکی افراد، اقدام به برداشت غیرمجاز از حسابشان می‌کنند.

اما نوع دیگر کلاهبرداری اینترنتی ارسال لینک به خصوص پیامک‌های قضایی است؛ در واقع با ایجاد ایجاد یک ترس و اطلاع از وضعیت اتهام قربانی را مجبور به باز کردن لینک می‌کنند. پس از کلیک بر روی این لینک ابتدا گوشی قربانی آلوده به نرم‌افزاری شده و پیامک‌هایی حتی برای شماره‌هایی که در گوشی فرد ذخیره نیستند هم می‌رود؛ سپس درخواست مقدار کمی پول برای اطلاع از وضعیت می‌شود که فرد با وارد کردن اطلاعات حساب خود موجودی حساب خود را از دست می‌دهد. پس از این اقدام، سپس شماره تلفن و کد ملی فرد را درخواست می‌کنند که با این کار کلاهبردار اقدام به فعال کردن همراه بانک قربانی می‌کند و چون به سامانه پیامکی هم دسترسی داره می‌تواند کد را بردارد و از حساب‌های فرد برداشت کند.

بنابراین مسئولان توصیه می کنند اگر پیامی ارسال شد که داخل آن لینکی فرستاده بود و برای دریافت خدماتی قرار بود پول بپردازید این پیامک جعلی است. پیامک‌های قوه قضاییه با سرشماره ADLIRAN است و اگر ADLIRAN در متن پیامک باشد این پیامک جعلی است ضمن اینکه اطلاع‌رسانی قوه قضائیه رایگان است.

در همین رابطه پلیس فتا چندی پیش در این زمینه هشدارهای لازم را در قالب ارسال پیامک به شهروندان داد. این سازمان در پیامک ارسالی خود به شهروندان توصیه کرده است هموطنان دریافت هر گونه تماس تلفنی با خطوط شخصی و پیام رسان ها مبنی بر دریافت جوایز در مسابقات رادیویی، خوش حسابی تلفن همراه و ... کلاهبرداری است؛ همچنین تحت هیچ شرایطی بر روی لینک‌هایی که از سرشماره های شخصی ارسال می شود کلیک نکنند.

گفتنی است طی دو ماه گذشته در این زمینه گفته شده بود مشترکین در صورت دریافت پیامک‌های مشکوک و حاوی لینک پرداخت رقم به هیچ وجه بر روی لینک کلیک نکنند و حتما به سر شماره دریافت پیامک توجه کنند چون قطعا نباید پیامک‌های از این نوع و اهمیت بالا با شماره شخصی برای افراد ارسال شده باشد. این مقام مسئول توصیه می کند، مشترکین به خاطر بسپارند که نهادهای دولتی و معتبر از سرشماره‌های شخصی اقدام به ارسال پیام نمی‌کنند و سازمان‌ها و نهادهای خصوصی و دولتی عمدتاً از شماره تلفن‌های پوششی موسوم به «number mask» مانند «police»، «adliran» و دیگر شماره‌های تحت عنوان مشخص و مورد تأیید برای اطلاع‌رسانی استفاده می‌کنند.

به صورت کلی کاربران باید توجه کنند که شخصی در شبکه‌های اجتماعی، دانلود نکردن فایل‌ها از سایت‌های نامعتبر و غیرمطمئن، به‌روزرسانی آنتی‌ویروس، دقت در وارد کردن نشانی درگاه‌های پرداخت الکترونیکی بانک‌ها و توجه به پروتکل امن HTTPS و عدم توجه به ایمیل یا لینک‌های

ناشناس از بروز و ظهور چنین کلاهبرداری‌هایی پیشگیری کرده و ضریب امنیت را در فضای مجازی افزایش می‌دهد.

منبع: ایسنا