گزارش خبر
NEWSREPORT

کد خبر: ۴۵۶۸۴۶
چهارشنبه ۱ تیر ۱۴۰۱ ۱۲:۳۶

سواستفاده از اعتماد مردم به برند پست؛

مراقب شیوه جدید کلاهبرداران اینترنتی باشید

«سلام، مامور اداره پست هستم. چون تازه اومدم منطقه شما آدرس خونتون رو نتونستم پیدا کنم. نامه قضایی دارین. شمارتونو از روی نامه برداشتم گفتم اطلاع بدم کد پیگیری روی نامتون ۱۷۳۰۰۶۵۲۸۹۱۰۹ بود. چون نامه سوم هست و اخطاریه آخر، اپلیکیشن پیگیری نامه قضایی رو براتون می‌فرستم پیگیری کنید»

به گزارش خبر شرکت ملی پست، شاید همین حالا که مشغول خواندن این متن هستید، پیامکی شبیه به آن را دریافت کنید. پیامکی که حاوی لینک آلوده به فیشینگ اطلاعات است و از سوی افرادی سودجو و به قصد خالی کردن حساب برای قربانی تنظیم و ارسال می‌شود. پیامکی که از چند روز گذشته تا همین امروز عامل خالی شدن حساب افراد بسیاری در سراسر کشور شده است.»
بی‌توجهی به نکات امنیتی و طرح این سؤال که چطور ممکن است مأمور اداره پست برای مشتری خود چنین پیامکی را تنظیم و لینک سامانه قضایی را ارسال کند، کلاهبرداری چند ده میلیونی را از افراد رقم زده است.
اگرچه تاکنون به مراتب گزارش‌هایی مشابه در قالب مطالب پیشگیرانه در صفحه حوادث روزنامه ها و حتی در شبکه های اجتماعی برای آگاه‌سازی شهروندان درباره شگرد جدید کلاهبرداری‌ها چاپ و منتشر شده است، اما همچنان افرادی هستند که در پی بی‌احتیاطی و بی‌توجهی به توصیه‌های پلیسی قطعه دیگری از پازل قربانی شدن در فضای مجازی را تکمیل می‌کنند.
نقشه‌های سودجویانه‌ای که در گذشته در قامت «برنده شدن در مسابقات تلویزیونی و رادیویی» ظاهر می‌شد، از چندی پیش با سواستفاده از برند پست و پستچی ، ردای «ابلاغیه‌های قضایی» را بر تن کرده است.
شاکی که مردی جوان است با در دست داشتن مرجوعه قضایی به مرکز پلیس فتای استان خراسان رضوی مراجعه کرد و مدعی شد که فردی با ادعای مأمور پست پیامکی را برایش ارسال و وی را از ابلاغیه قضایی مطلع کرده است.
مال‌باخته بر روی لینک ابلاغیه قضایی که همان فرد برایش ارسال کرده می‌زند و نرم‌افزار مورد نظر را نصب می‌کند.
بعد از نصب، نرم‌افزار دسترسی‌ها به گوشی تلفن همراه را از مرد جوان می‌خواهد و او هم بی‌اطلاع از همه‌جا با دست خودش اجازه می‌دهد تا گرداننده اصلی نرم‌افزار اطلاعات خصوصی‌اش را برداشت کند.
از آنجا که شاکی همچنان در پی دریافت متن ابلاغیه قضایی‌اش بوده برای اطلاع از آن به ظاهر حق عضویت ناچیزی را طبق درخواست نرم‌افزار پرداخت می‌کند که همین عمل موجب رقم خوردن سرقت از وی می‌شود.
جاسوس‌افزار که نقش خود را خوب ایفا کرده اطلاعات بانکی طعمه خود را در اختیار سارقان قرار می‌دهد و از آنجا که متهمان دسترسی کامل به سرویس پیام‌های گوشی تلفن همراه شاکی پیدا کرده‌اند، پس از دریافت رمز دوم نقشه شیادانه خود را عملی می‌سازند و ۴۷ میلیون تومان پول بی‌زبان قربانی را به جیب می‌زنند. شاکی تا به خودش بیاید در یک چشم برهم زدنی پول‌هایش به چند کارت بانکی سرازیر و در نهایت هم تبدیل به رمزارز و خرید کالا از سایت‌های واسطه‌گر می‌شود.
توجه داشته باشید شرکت ملی پست تمامی پیام های اطلاع رسانی خود را از تارنمای خود به نشانی post.ir و صفحات رسمی خود در پیام رسان های گپ وسروش به نشانی natuinalpost و شبکه اجتماعی اینستاگرام به نشانی irannationalpost اعلام خواهد کرد.
همچنین لازم به ذکراست این شرکت هیچگونه پیامک و درخواستی مبنی بر ورود به لینک و مشاهده وضعیت مرسوله یا ابلاغیه برای مشتریان به هیچ طریقی ارسال نمی کند.
با افزایش سواد رسانه ای خود و آگاهی بخشی در میان اقشار مختلف از سواستفاده های احتمالی کلاهبرداران اینترنتی درامان باشیم.