ZENDEGI-SALAM
ضمیمه روزنامه خراسان
دو شنبه • ۲۴ مرداد ۱۴۰۱
۱۷ محرم ۱۴۴۴ • ۱۵ آگوست ۲۰۲۲
شماره ۲۱۰۰۸
۲۲۲۸

تازه‌ترین ترفندهای کلاهبرداران پیامکی

ماجرای خبرساز خالی کردن حساب افراد با پیامک جعلی قطع یارانه در چند روز اخیر، بهانه‌ای شد از متداول‌ترین شیوه‌های کلاهبرداری پیامکی بگوییم

مجید حسین‌زاده | روزنامه‌نگار

پرونده

خیلی خوب بلدند که متن پیامک را چطور تنظیم کنند تا آرامش و قرار را از ذهن شما بگیرند و تا زمانی که روی لینک ارسالی‌شان کلیک نکنید، آرام نگیرید! شخصا هم تجربه این اتفاق را داشتم. در حال استراحت بودم که چنین پیامکی که تصویرش را هم می‌بینید، برایم آمد: «شکواییه‌ای علیه شما در سامانه قضایی قرار گرفته است. رهگیری از سامانه زیر: .... عدم پیگیری، جلب می‌باشد». با این که هزاران بار شنیده بودم که چنین پیامک‌هایی اگر از شماره شخصی ارسال شده باشد، اعتباری ندارد و مطمئن بودم که دلیلی برای شکایت از من وجود نداشته، اما باز هم استرس عجیبی وجودم را فرا گرفت و تا قبل از زمانی که آدرس سایت سامانه قضایی را جست و جو کردم و متوجه شدم که آدرس سایتی که در این پیامک نوشته شده مربوط به قوه قضاییه نیست، آرامش نداشتم. از آن طرف کنجکاو هم بودم که روی لینک کلیک کنم تا ببینم به کجا می‌رود که دست آخر هم بعد از چند ساعت، بالاخره کلیک کردم اما وقتی به صفحه‌ای برای دریافت اطلاعات کارت بانکی و شماره تلفن همراهم هدایت شدم، دیگر جلوتر نرفتم! به تازگی هم یک پیامک جعلی به مشترکان ارسال می‌شود که یارانه شما قطع شد، اطلاعات بیشتر در سایت ..... در پرونده امروز زندگی سلام به متداول‌ترین شیوه‌های کلاهبرداری پیامکی که در چند وقت اخیر خبرساز شده، خواهیم پرداخت.

ارسال محرمانه رمز عبور جدید برای حساب بانکی جدید!

در بسیاری از شیوه‌های کلاهبرداری، طعمه‌شان را با پول وسوسه می‌کنند. یکی از جدیدترین روش‌های کلاهبرداری واتس‌اپی، این است که یک پیام از یک حساب جدید که تقریبا ۳۰۰ هزار تومان پول در آن است، برای شما ارسال می‌شود. در این پیام، علاوه بر نام کاربری و رمز عبور، به موجودی فعلی حساب هم اشاره شده و از شما درخواست می‌شود که این اطلاعات محرمانه را با دیگران به اشتراک نگذارید! در این شرایط که شما به این پیامک و محتوای آن حساس شده‌اید و بعد از کلیک شما روی لینک، گوشی‌تان به یک بدافزار آلوده می‌شود و یک سری اطلاعات شخصی‌تان در معرض سوء استفاده قرار خواهد گرفت.

در خواست برای قطع نشدن یارانه و خالی شدن حساب!

در جدیدترین مورد از کلاهبرداری های پیامکی که در چند روز اخیر خبرساز شده، پیامکی به دست بعضی از افراد رسیده که یارانه‌تان قطع شد و برای اعتراض باید، اطلاعات‌تان را در یک لینک ثبت کنید تا بررسی شود. در این روش از کلاهبرداری مجرمان سایبری با ارسال پیامک قطعی یارانه و درخواست ثبت اطلاعات بانکی، این اطلاعات را به سرقت می برند و به برداشت غیرمجاز از حساب آن‌ها اقدام می کنند.

پیامک جعلی از ثبت شکایت در قوه قضاییه

در این روش، مجرمان سایبری با جعل کردن آدرس اینترنتی سامانه ثبت نام الکترونیک قوه قضاییه، اقدام به کلاهبرداری از کاربران فضای مجازی می کنند. این پیامک‌ها حاوی مطالبی از قبیل: ثبت شکواییه، ابلاغ حکم و ... است که کاربران فضای مجازی به دلیل استرس ایجاد شده و کنجکاوی به آدرس (لینک) جعلی که در متن پیام است مراجعه می کنند و با درخواست کسر وجه و ثبت اطلاعات بانکی توسط شهروندان از حساب کاربران برداشت غیرمجاز می‌شود. همین جا لازم است با وجود اعلام چندباره پلیس و دستگاه قضایی در خصوص این پیامک‌های جعلی مجدد تاکید شود پیامک‌های ابلاغ قضایی فقط با سر شماره ADLIRAN ارسال می‌شود و هر گونه پیامک دارای لینک، جعلی و به قصد کلاهبرداری است. اما شاید بپرسید که وقتی شما روی این لینک کلیک کنید، چه اتفاقی می افتد؟ اگر اطلاعات‌تان را وارد نکنید، باز هم خطرناک است؟

گوشی که به بدافزار آلوده می‌شود | به طور مثال و در یک پرونده قضایی که متهمش به تازگی هم دستگیر شده، فرمانده انتظامی شهرستان دشتستان این طور توضیح داده: «در این روش کلاهبرداری که در پوشش سامانه ابلاغ الکترونیکی قوه قضاییه (سامانه ثنا) است، مشخص شد که فردی کلاهبردار اقدام به ارسال پیامکی با عنوان «علیه شما در دادسرای عمومی و انقلاب شکایت شده، جهت مشاهده متن شکواییه می‌توانید از طریق لینک زیر اقدام کنید» کرده که حاوی لینک جعلی بوده است و به محض کلیک کردن قربانی برای مشاهده شکواییه، گوشی وی آلوده به یک بدافزار می‌شود. پس از آلوده شدن گوشی قربانی دو اتفاق مهم رخ می‌دهد که در مرحله نخست همین پیامک از شماره همراه قربانی به صورت انبوه برای افرادی دیگر ارسال می شود و دیگران را در این چرخه کلاهبرداری دخیل می کند. در مرحله بعد زمانی که قربانی برای مشاهده شکواییه خود وارد لینک معرفی شده می‌شود باید مبلغی اندک مثل دو هزار تومان را پرداخت کند که در این زمان به درگاه پرداخت جعلی بانکی هدایت می شود و اطلاعات بانکی وی به سرقت می‌رود؛ در این پرونده از حساب قربانی به همین روش مبلغ ۸۰۰ میلیون ریال برداشت غیرمجاز صورت گرفته است. پس از بررسی‌های لازم متهم که خانمی ۱۹ ساله و ساکن یکی از استان‌های مرکزی کشور بود، شناسایی، دستگیر و تحویل مقام‌های قضایی شد».

این ۷ توصیه ساده را جدی بگیرید

۱ فیشینگ، جعل هویت یک سایت معتبر از سوی کلاهبرداران است. آن‌ها با طراحی پیام‌هایی خاص و ارسال آن به صورت ایمیل یا پیامک، کاربران را ترغیب به ورود به صفحه پرداخت جعلی می کنند. برای جلوگیری از فیشینگ، حتما به آدرس در گاه پرداخت‌مان توجه کنیم. shaparak.ir درگاه اصلی پرداخت بانک مرکزی است. بعضی از شیادان با اضافه کردن یک حرف به این آدرس اینترنتی، می کوشند تا با سایتی که به چشم کاربر طبیعی می‌آید، اطلاعات بانکی او را به دست بیاورند.

۲ سایت‌های امن در آدرس بار مرورگر علامت قفل دارند یا با حروف https شروع می‌شوند. سایت‌های پرداختی که این نشانه‌ها را ندارند، سایت‌های امن محسوب نمی‌شوند و احتمال فیشینگ در آن‌ها بسیار زیاد است.

۳ سایت های معروف خرید و فروش از جمله محبوب‌ترین پلتفرم‌ها برای فیشرهاست. هیچ سازمان و نهاد دولتی با شماره شخصی برای شما پیامک ارسال نمی کند (پیامک‌هایی با موضوع سامانه ثنا، یارانه و...).

۴ هنگام نصب اپلیکیشن به دسترسی‌های اپلیکیشن (به ویژه دسترسی پیامک) خیلی دقت کنید و روی این دسترسی بسیار حساس باشید. فکر نکنید اگر حواس‌تان به رمز کارت و درگاه هست کار تمام است. با نصب اپلیکیشن کلاهبردار ممکن است از خط شما برای ۲۵۰ نفر دیگر پیامک کلاهبرداری را ارسال کند!

۵ پیامک جعلی دو مشخصه مهم دارد. ابتدا این که این پیامک‌ها با سر شماره معمولی ارسال می‌شود و دیگر مشخصه لینک موجود در پیامک است. شهروندان باید بدانند تنها سر شماره پیامک‌های قوه قضاییه Adliran است و برای پلیس فتا با police Fata ارسال می‌شود. همچنین تنها سامانه‌ای که در پیامک‌های قوه قضاییه معرفی می‌شود که به آن رجوع کنند سامانه ثناست.

۶ لینک موجود در پیامک‌های جعلی کاربر را به درگاه پرداخت الکترونیکی هدایت می کند و در ازای مبلغ ناچیز رمز دوم را می‌خواهد که معمولا در بار اول رمز را قبول نمی کند و می گوید اشتباه است. در صورتی که رمز دوم کاربر اشتباه نیست و کلاهبردار با این کار زمان می‌خرد تا بتواند از حساب قربانی پول خارج کند.

۷ در هیچ برنامه مشکوکی ثبت نام نکنید حتی برای تخفیف. اگر برنامه‌ها یا سایت‌هایی اطلاعات بیشتر از آن چه برای خرید شماست از شما می‌خواهند به آن‌ها باید مشکوک شوید. در بسیاری از موارد ممکن است اطلاعات شما را به طرف سومی بفروشند. دقت داشته باشید که قبل از دادن هرگونه اطلاعات به یک وب‌سایت نگاهی به سیاست حفظ حریم خصوصی آن داشته باشید.

فرصت ۲۴ ساعته تا دریافت سود سهام عدالت

مجرمان سایبری با ارسال پیامک یا پیام در شبکه‌های اجتماعی با نام واریز سود سهام عدالت مترصد کلاهبرداری از مردم هستند. پیام‌های جعلی که به تازگی هم منتشر شده، از مخاطبان درخواست می کند که برای دریافت سود سهام خود از طریق لینک آلوده اقدام کنند که سهامداران باید از این اقدام کلاهبردارانه آگاه باشند. در متن وسوسه کننده این پیامک برای کلیک روی لینک جعلی نوشته شده که برای دریافت سود ۲۲ میلیون ریالی سهام‌عدالت خود از طرف هیئت وزیران کشور، ۲۴ ساعت فرصت دارید تا روی لینک، کلیک کنید!

در آرزوی دریافت اینترنت رایگان و شارژ فوق‌العاده

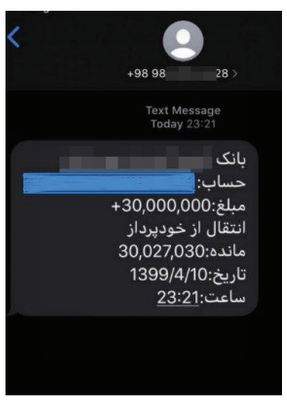
به هیچ‌وجه به لینک‌های ارسالی در کانال‌ها و شبکه‌های اجتماعی و همچنین پیامک‌هایی با عنوان ثبت‌نام و دریافت اینترنت رایگان توجه نکنید، زیرا بیشتر آن ها دارای لینک‌های جعلی است. همچنین به هیچ عنوان در این گونه قرعه کشی‌ها شرکت نکنید، چرا که این احتمال وجود دارد که به محض شرکت در چنین قرعه کشی هایی، اطلاعات تلفن همراه‌شان هک و حساب‌های بانکی‌شان توسط مجرمان تخلیه شود. کلاهبرداری با پیشنهاد خرید شارژ فوق‌العاده هم در فضای مجازی زیاد دیده می‌شود. مجرمان در این روش با ایجاد سایت جعلی و وعده فروش شارژ به همراه هدیه، اطلاعات حساب بانکی افراد را به دست می‌آورند.

نصب یک نرم‌افزار برای پیگیری شکایت پلیس از شما!

چند وقت پیش، یک پیامک جعلی با عنوان شکایت پلیس را هور برای برخی از رانندگان ارسال شد که در آن از شهروندان درخواست می کرد برای پیگیری موضوع وارد یک لینک جعلی شوند. این پیامک‌ها از شماره‌های ناشناس ارسال می شد، کاربر را به یک سایت مشکوک و جعلی هدایت و در انتها از کاربر درخواست می کرد یک اپلیکیشن ناشناس را نصب کند. سپس در این نرم‌افزار، اطلاعات و سیله نقلیه فرد و حسابش هدف سوء استفاده مجرمان سایبری قرار می گرفت.

واریزهایی که سراب است!

در این شیوه از کلاهبرداری، پیامکی از واریز پول برای‌تان ارسال می‌شود که در لحظه اول احتمالا شما را هیجان‌زده می کند. بعد از دریافت این پیامک، با شما تماس گرفته می‌شود که مبلغ، اشتباهی به حساب شما واریز شده و پول را به شماره کارتی که اعلام می‌شود، برگردانید. این در حالی است که پیامک واریز وجه اصلا از سامانه پیامکی بانک ارسال نشده و از شماره تلفنی متفرقه ارسال شده است که البته ظاهرا کلاهبرداران برای فریب بیشتر از شماره تلفن‌های نسبتا رندو با تکرار چند صفر پشت سر هم استفاده می کنند تا به خیال‌شان اختلافی میان این پیامک با پیامک‌های بانک به نظر نرسد.



گول زدن به بهانه رجیستری تلفن همراه

پس از اجرای طرح رجیستری، ارسال پیامک‌هایی به اسم همتا به همراه آدرس‌های جعلی و صفحه‌هایی که مانند سامانه همتا طراحی شده، اتفاق تازه‌ای نیست اما هر بار به روشی صورت می گیرد. پیش از این بارها اتفاق افتاده که پیامکی برای برخی افراد ارسال و از آن‌ها خواسته شده برای جلوگیری از قطع شدن تلفن همراه، مبلغی را پرداخت کنند. بنابراین پیامک ارسالی با مضمون «دستگاه تلفن شما قانونی است ولی فعال نشده و برای جلوگیری از قطع شدن شبکه موبایل تا ۲۴ ساعت جهت فعال سازی اقدام نمایید» جعلی و ترفند سودجویان برای کلاهبرداری اینترنتی است.

از ثبت نام طرح معیشتی تا سهمیه سوخت و...

ماجرای پیامک‌های جعلی به همین جا ختم نمی‌شود. «ثبت نام برای سهام عدالت، یارانه و طرح معیشتی»، «آزادسازی سهام عدالت»، «ثبت نام در سامانه سجام»، «ثبت نام سهمیه یا کارت سوخت»، «افزایش سهمیه سوخت مسافربرهای اینترنتی» و ... از جمله موضوعاتی هستند که تاکنون دستمایه کلاهبرداری‌های پیامکی شده‌اند. همچنین به تازگی افراد سودجو با ارسال پیامک به صورت انبوه به هموطنان با عنوان «بسته حمایتی دولت به مبلغ ۲۴۵۰۰۰ تومان» از طریق درگاه بانکی جعلی اقدام به کلاهبرداری کردند.