رئیس سابق شورای‌عالی فضای مجازی:

شرایط اقتصادی یکی از دلایل کلاهبرداری اینترنتی است

سیدجواد نژادموسوی
روزنامه‌نگار

گفت و گو

رئیس سابق شورای‌عالی فضای مجازی معتقد است کلاهبرداری اینترنتی و فیشینگ تنها مختص ایران نبوده و بسیاری از کشورها کم‌وبیش درگیر این مشکل هستند و برای مقابله با این پدیده باید چند اتفاق به صورت هم‌زمان رخ دهد. سید ابوالحسن فیروزآبادی در این باره با «آتیه‌نو» گفت‌وگویی داشته که در ادامه از نظر می‌گذرانید.

• موضوع کلاهبرداری‌های اینترنتی، فیشینگ و انواع تخلفات و سرقت‌های این‌چنینی با ترفندهای مختلف مطرح می‌شود، در حال حاضر در چه وضعیتی قرار داریم و علت این آسیب‌پذیری را چه می‌دانید؟

فیشینگ یکی از روش‌های کلاهبرداری است که در دنیا به‌صورت گسترده استفاده می‌شود و تنها محدود به ایران یا یکی دو کشور نیست. این روش هنوز برای کلاهبرداران مؤثر و به‌صرفه است. البته در کشور تمهیداتی برای مقابله با فیشینگ و کلاهبرداری‌های اینترنتی اندیشیده شده و این کار برعهده پلیس فتاست. در این راستا زیرساخت‌های لازم در اختیار پلیس فتا قرار داده شده تا بتواند از این‌گونه کلاهبرداری‌ها جلوگیری کند.

در این میان مردم نیز باید بیش از پیش توجیه شده و آموزش داده شوند؛ چراکه در زمینه آموزش‌های مرتبط با سواد فضای مجازی و سواد اینترنتی کم‌کاری‌هایی دیده می‌شود. در حالی که حتی در مدارس باید واحد درسی برای چنین مسائلی تخصیص دهیم. درسی با این سرفصل در مدارس ما وجود ندارد، اما در کشورهای توسعه‌یافته و در حال توسعه از همان ابتدای دوران آموزشی این موضوعات به کودکان آموزش داده می‌شود.

به نظر من مسئله فیشینگ جزو آن دسته مشکلاتی است که درگیر آن هستیم و خواهیم بود. به نظر نمی‌رسد که آمار فیشینگ و کلاهبرداری اینترنتی در ایران بالاتر از سایر کشورها باشد، اما به هر حال وجود دارد.

بخش آگاهی‌رسانی و ترویجی در زمینه فیشینگ و انواع کلاهبرداری‌های اینترنتی باید بیشتر از گذشته شود تا مردم کمتر درگیر این معضلات و پیامدها و خسارات ناشی از آن شوند.

• گرچه در همه کشورها شاهد فیشینگ و کلاهبرداری‌های اینترنتی هستیم، اما در ایران اطلاعات و موضوعات جذابی برای مردم وجود دارد که معمولاً بیشتر از موضوعات دیگر دستخوش فیشینگ است که از این میان می‌توان به یارانه‌ها، سهام عدالت و... اشاره کرد. به نظر شما چه اقداماتی باید برای کاهش آمارها در این حوزه انجام شود؟

لازم است به این موضوع توجه ویژه شود که شرایط اقتصادی کشور به‌دلیل اعمال تحریم‌های ظالمانه دچار نوساناتی شده است. در کشورهای توسعه‌یافته یا در حال توسعه نوسانات اقتصادی به‌شدت کشور ما نیست و این عدم تعادل‌ها در بازار نابه‌سامانی ایجاد می‌کند. به‌عنوان مثال گوشی آیفون یا برخی دیگر از کالاها خاص می‌شوند و مردم برای اینکه بتوانند سود بیشتری ببرند، جذابیت چنین مسائلی برای آن‌ها بیشتر شده و همین مسئله دقت آن‌ها را کاهش می‌دهد.

روش‌های مختلفی برای کلاهبرداری اینترنتی وجود دارد که یکی از آن‌ها فیشینگ است. در حال حاضر تنوع کلاهبرداری‌هایی که در کشور مورد استفاده متخلفان قرار می‌گیرد، نسبت به کشورهای دیگر بالاست و فقط محدود به فضای مجازی نمی‌شود. در فضای فیزیکی هم شاهد کلاهبرداری‌هایی از جمله صندوق‌های نامعتبر، ثبت‌نام‌های نامعتبر و موارد مشابهی از این دست هستیم.

بنابراین به نظر می‌رسد شرایط تحریم در بروز چنین تخلفات و کلاهبرداری‌هایی در کشور، بی‌تأثیر نیست و امیدواریم این موضوع نیز حل شود.

• با توجه به اینکه سابقه عضویت و ریاست شورای‌عالی فضای مجازی را داشتید، آیا در این شورا، گزارش یا آماری از میزان وقوع کلاهبرداری‌های اینترنتی و فیشینگ تهیه و تدوین شده است؟ یا اینکه آیا تاکنون بررسی شده که تا چه اندازه این موضوع بر اقتصاد کشور اثرگذار است؟

از آنجا که حجم کلاهبرداری‌های اینترنتی و به‌ویژه فیشینگ کم و ناچیز است، اثری روی اقتصاد کشور ندارد، اما تعداد افرادی که از این موضوع آسیب‌دیده و متضرر شده‌اند قابل توجه است. به‌صورت معمول در این نوع تخلفات اعداد و ارقامی که دستخوش کلاهبرداری قرار می‌گیرد، چندان زیاد نیست و بیشترین فیشینگی که صورت می‌گرفت در رابطه با رمز کارت بانکی بود که در شورای‌عالی فضای مجازی به این مسئله وارد شده و رمز پویا را در کشور پیاده‌سازی کردیم. پس از آن در تمام انواع کلاهبرداری‌های اینترنتی از جمله فیشینگ در ایران افت شدید و قابل توجهی را شاهد بودیم که نشان می‌داد ایجاد و راه‌اندازی رمز دوم پویا به خوبی توانسته نقش خود را در برابر کلاهبرداری‌های اینترنتی ایفا کند.

در آخرین آمارهایی که در سال گذشته از فیشینگ و انواع کلاهبرداری‌های اینترنتی تهیه و تنظیم کردیم، ایران تقریباً در ردیف کشورهای خوب قرار گرفت. در حالی که پیش از راه‌اندازی رمز دوم پویا ده‌ها هزار پرونده کلاهبرداری اینترنتی و فیشینگ داشتیم و به یک‌باره سقوط شدید در این زمینه به وجود آمد. البته تلاش‌های پلیس فتا نیز در این زمینه قابل تقدیر است.

• آیا در همان زمانی که در شورای‌عالی فضای مجازی بودید، آمار کلاهبرداری اینترنتی و فیشینگ در حوزه سهام عدالت و یارانه‌ها آن‌قدر بالا بود که بتوان گفت یکی از مسائل و بخش‌هایی است که بیشترین پرونده را پس از رمز کارت بانکی به خودش اختصاص داده و می‌شود فکری کرد تا مردم هر لینک و پیامی به دست‌شان می‌رسد را باز نکنند؟

بعید است آمار بالایی از فیشینگ و کلاهبرداری اینترنتی به پیام‌های مرتبط با یارانه و سهام عدالت وجود داشته باشد و تا جایی که اطلاع دارم و تا سال گذشته که در شورای‌عالی فضای مجازی عضویت داشتم، چنین گزارشی با این مضمون به دست ما نرسیده بود. مردم بایستی آگاه‌تر از گذشته شوند؛ چراکه حتی پیام‌های قوه قضاییه نیز دستخوش فیشینگ شده و مردم به گمان اینکه این پیام از سوی قوه قضاییه است، مورد سوءاستفاده و کلاهبرداری قرار می‌گیرند. این نشان می‌دهد که کلاهبرداران به‌دلیل منافع اقتصادی، شهامت نسبتاً بالایی دارند. بنابراین مردم باید آموزش کاملی در این زمینه ببینند تا مورد حمله فیشینگی قرار نگیرند.

• اگر بخواهید توصیه‌ای به مردم داشته باشید تا از حملات فیشینگ در امان باشند و در دام کلاهبرداران اینترنتی نیفتند، به چه نکاتی اشاره می‌کنید؟

مهم‌ترین نکته این است که اگر مسائلی درباره تشویق‌ها، جوایز و هدایا مطرح می‌شود، مردم بدانند که در این زمینه احتمال کلاهبرداری وجود دارد. در هرگونه تلفن، پیامک یا اقدامی که می‌خواهند برای جابه‌جایی پول انجام دهند بایستی دقت لازم را داشته باشند تا مورد کلاهبرداری و حمله فیشینگ قرار نگیرند. همچنین به نام‌ها و لوگوها توجه بیشتری کنند تا کاری که انجام می‌دهند صحیح باشد.

فیشینگ چگونه حساب مردم را خالی می‌کند؟

گزارش

فیشینگ یکی از انواع کلاهبرداری اینترنتی است و برای جمع‌آوری اطلاعات شخصی افراد با استفاده از ایمیل‌ها و وب‌سایت‌های فریبنده دست به کار می‌شود. همچنین فیشینگ یکی از رایج‌ترین حملات سایبری محسوب می‌شود.

به گفته کارشناسان آی‌تی و متخصصان حوزه امنیت سایبری، یکی از ویژگی‌های قابل توجه فیشینگ، عنصر سورپرایز است. این ایمیل‌ها زمانی دریافت می‌شوند که قربانی انتظارش را ندارد. مهاجمان می‌توانند ایمیل‌ها را زمان‌بندی کنند تا قربانیان در شرایط حواس‌پرتی با چیزهای دیگر مانند کار، آن‌ها را دریافت کنند. تمرکز و توجه دائمی به ایمیل‌های مشکوک غیرممکن است و کلاهبرداران این موضوع را خوب می‌دانند.

در حمله فیشینگ، هکرها از ارتباطات نوشتاری (ایمیل یا پیام فوری) برای سرقت اطلاعات شخص به‌عنوان یک منبع معتبر استفاده می‌کنند. در واقع هدف این است که گیرنده ایمیل فریب خورده و با تصور اینکه پیام مورد نظر چیزی است که او می‌خواهد، روی لینک کلیک کرده و یا پیوست را بارگذاری کند. آن‌طور که در خبرهای بین‌المللی آمده، گزارش سالانه جرائم اینترنتی (FBI) در سال ۲۰۲۰ نشان می‌دهد، حملات فیشینگ ۳۲٫۳۵ درصد از کل حملات سایبری سال ۲۰۱۹ را شامل می‌شده که در واقع بیشترین حمله بوده و ۲۴۱ هزار و ۳۴۲ مورد فیشینگ رخ داده است. این رقم در پنج سال بیش از ۱۰ برابر شده، در حالی که در سال ۲۰۱۵ این رقم ۱۹ هزار و ۴۶۵ مورد بوده است.

طبق بررسی‌ها اکثر حملات فیشینگ از طریق ایمیل انجام می‌شود. مهاجم به احتمال زیاد با لیستی از ایمیل‌های نقض شده اقدام کرده و ایمیل‌های فیشینگ را به‌صورت عمده ارسال می‌کند و انتظار دارد حداقل بخشی از لیست مورد نظر را فریب دهد.

گول هکرها را نخورید

در ایران نیز با توجه به موارد و نیازمندی‌های جذاب، هکرها یا همان مهاجمان از آن برای فریب مردم استفاده می‌کنند. از جمله این نیازمندی‌ها یارانه‌های نقدی و معیشتی، سهام عدالت، سهمیه‌بندی بنزین، جوایز و هدایای بانکی و غیره است که هکرها با طراحی ایمیل، پیامک یا سایتی مشابه آن، مردم را با استفاده از روش‌های مختلف به سمت لینک‌های مخرب و جعلی می‌کشانند تا بتوانند از غفلت آن‌ها سوءاستفاده کرده و اطلاعات‌شان را سرقت کنند.

حتی اخیراً پیامک‌هایی به نام قوه قضاییه از سوی این هکرها برای مردم ارسال می‌شود و مردم نیز به خیال واقعی بودن پیامک، لینک مورد نظر را باز می‌کنند. این دقیقاً همان موقعیتی است که هکرها می‌خواهند و حملات فیشینگی دقیقاً از همین لحظه آغاز شده است.

البته در این میان سازمان‌ها و نهادهای مختلف که از نام‌شان سوءاستفاده می‌شود، بارها و بارها در پیام‌ها و اطلاعیه‌های مختلف از مردم خواسته‌اند تا پیام‌هایی که به نام آن‌ها برای‌شان ارسال می‌شود را باز نکنند. از سوی دیگر پلیس فتا به‌عنوان نهاد متولی برای مقابله با این دست کلاهبرداری‌ها هشدارهای متعددی به مردم داده است. کارشناسان و حقوق‌دانان این حوزه معتقدند که اعمال نظارت‌های مؤثر در فرایند ثبت شرکت‌ها، اعتبارسنجی مؤسسان مراکز تجاری و افزایش سواد رسانه‌ای مخاطبان عمومی در زمینه جلوگیری از کلاهبرداری‌های اینترنتی مؤثر است.

در باز کردن لینک سختگیر باشید

حجت‌الاسلام نجفی، معاون اجتماعی و پیشگیری از وقوع جرم دادگستری کل استان سیستان و بلوچستان در این‌باره می‌گوید: «هر پیام دریافتی در پیام‌رسان‌های موبایلی با عناوین دریافت سود سهام عدالت با هدف کلاهبرداری و خالی کردن حساب بانکی مخاطبان فرستاده می‌شود. ضمن اینکه شهروندان مطلع باشند که هر پیام دریافتی از شماره‌های شخصی و یا پیام‌رسان‌های موبایلی با موضوع شکایت قضایی به قصد کلاهبرداری و سرقت از حساب بانکی آنان است و پیامک‌های قوه قضاییه صرفاً با سرشماره (ADLIRAN) برای مخاطبان ارسال می‌شود. علاوه بر این هرگز پیامک‌های ارائه خدمات دولتی نظیر ابلاغ الکترونیک، سامانه ثنا، دریافت یارانه، طرح‌های معیشتی، سود سهام عدالت و انواع قبوض از سرشماره‌های شخصی و یا شماره تلفن همراه برای مخاطبان ارسال نمی‌شود.»

بر این اساس لازم است در صورت دریافت پیامک یا ایمیل‌های مشکوک حاوی لینک آدرس، از باز کردن آن اجتناب و از ارسال این محتوا به سایر افراد خودداری شود. علاوه بر این یکی از مصادیق پرتکرار کلاهبرداری در سال‌های اخیر در حوزه رمزارزها و متاورس انجام گرفته، لذا باید بدانیم که فروش رمزارزهای جعلی یا شبیه‌سازی شده از شگردهای رایج کلاهبرداران حرفه‌ای است. با توجه به این امر که بازار ارزهای دیجیتال یک بازار نوپا محسوب می‌شود، حتماً قبل از فعالیت در این بازارها، ضرورت دارد تا آموزش‌های لازم از منابع معتبر اخذ شود تا سرمایه شهروندان از بین نرود. در واقع تبلیغات فریبنده برای دریافت سودهای نجومی در سرمایه‌گذاری بر روی ارزهای دیجیتال از شیوه و شگردهای رایج کلاهبرداری است.

اصرار به پرداخت بیعانه

سرهنگ داوود معظمی گودرزی، رئیس پلیس فتای پایتخت با بیان اینکه طمع و بیعانه دو کلیدواژه اصلی کلاهبرداری رایانه‌ای است، می‌گوید: «کلیدواژه اصلی جلوگیری از سرقت و کلاهبرداری در این سایت‌ها پرداخت بیعانه و به طمع انداختن افراد است. شهروندان به‌هیچ عنوان اعتماد نکنند و بدانند تمام کسانی که در این سایت‌ها کلاهبرداری می‌کنند اصرار به پرداخت بیعانه دارند. در عمده آگهی‌های کلاهبرداری معمولاً قیمت را پایین می‌گذارند و یا خود را فردی با جایگاه بالا معرفی می‌کنند و بیشتر آدرس محله‌های بالای شهر را می‌دهند تا افراد با اعتماد و طمع، بلافاصله کالا را خریداری یا بیعانه را پرداخت کنند.»

در چنین شرایطی مردم باید دقت داشته باشند که از فروشگاه‌های اینترنتی دارای نشان اعتماد الکترونیک خرید کنند. همچنین عدم پرداخت بیعانه در خرید از سایت‌های واسط یا شبکه‌های اجتماعی، عدم اطمینان به نتایج نشان داده شده در موتورهای جست‌وجوگر، توجه به آدرس صحیح درگاه پرداخت اینترنتی و جعلی نبودن آن حائز اهمیت است. جهت پیشگیری از کلاهبرداری به شیوه رسید جعلی، شهروندان و کسبه از تحویل کالا قبل از دریافت پیامک واریز وجه خودداری کنند. بهتر است در خرید اینترنتی با دقت لازم از سایت‌ها و فروشگاه‌های معتبر که نماد اعتماد الکترونیکی دارند خرید انجام شود.

نکته

چگونه از فیشینگ در امان بمانیم؟

کامبیز میزانیان
مدرس دانشگاه صنعتی شریف و کارشناس (IT) و (ICT)

فیشینگ در واقع نوعی کلاهبرداری است که با مشابه‌سازی سایت یا اپلیکیشنی که مردم از آن استفاده می‌کنند، اقدام به سرقت اطلاعات مورد نیاز برای انجام سرقت می‌کند. یعنی سایتی دقیقاً مشابه (از نظر شکل ظاهری) سایتی که مردم معمولاً به آن مراجعه می‌کنند، (مانند سایت یک بانک خاص) طراحی می‌شود و به نحوی مردم را به سمت آن سایت تقلبی یا کپی هدایت می‌کند. مردم هم متوجه نمی‌شوند که این سایت اصطلاحاً فیک است؛ چراکه احتمال دارد تنها یکی از حروف موجود در آدرس سایت آن بانک با سایت اصلی متفاوت باشد. بنابراین به‌دلیل شباهت بسیار زیاد آدرس اینترنتی و به‌خصوص شکل و قالب سایت نسبت به سایت اصلی، کاربر با تصور اینکه وارد سایت بانک مورد نظر خود شده، اطلاعات حساب و کارت بانکی‌اش را در اختیار سایت تقلبی قرار می‌دهد و دقیقاً از همین نقطه فیشینگ آغاز می‌شود؛ چراکه طراح سایت جعلی با اطلاعاتی که از کاربر دریافت کرده وارد سایت اصلی می‌شود.

با توجه به شرایط اقتصادی موجود در کشور و موضوعات جذابی مانند یارانه، سهام عدالت، هدایای بانکی و مواردی از این دست، از همین مسئله برای تله‌گذاری و سرقت اطلاعات مردم از طریق فیشینگ استفاده می‌شود. برای مصون ماندن از فیشینگ یا دیگر اقسام کلاهبرداری‌های اینترنتی می‌توان گفت که طراحان سایت تقلبی مورد نظر، مردم را به‌وسیله مهندسی اجتماعی یعنی جلب نظرشان از راه‌های مختلف به سمت‌وسوی این سایت می‌کشانند. این کار از طریق پیام‌ها، پیامک‌ها و ایمیل‌های ارسالی رخ می‌دهد.

وقتی در این زمینه از مهندسی اجتماعی صحبت می‌کنیم به معنای جذاب شدن سایت تقلبی با استفاده از پیام‌ها و ایمیل‌های ارسالی است. حتی در مواردی، بخشی از اطلاعات کاربران را در اختیار دارند. به‌عنوان مثال ممکن است اسم یک کاربر یا بخشی از اطلاعات شخصی و هویتی او را داشته باشند و از آن در پیامک ارسالی استفاده کنند، اما در کنار آن اطلاعات، متنی ترغیب‌کننده برای باز کردن لینک پایین متن نوشته شده است.

در این میان ذکر چند نکته به عنوان توصیه‌های مهم به مردم و برای جلوگیری از حملات فیشینگی ضروری به نظر می‌رسد. در وهله نخست مردم باید توجه داشته باشند که به لینک‌هایی که از طریق شبکه‌های اجتماعی، پیامک یا ایمیل برای آن‌ها ارسال می‌شود وارد نشوند.

در این مرحله باید اصالت یک پیام را بررسی و راستی‌آزمایی کنند و ببینند که سرشماره‌ای که برای آن‌ها پیامک ارسال کرده با سرشماره آن دستگاه متولی یکی است یا خیر؟ مثلاً سرشماره قوه قضاییه عدل ایران است. یا اگر ایمیلی برای آن‌ها ارسال شده، قبل از باز کردن اگر به آدرس فرستنده ایمیل نگاهی اجمالی بیندازند، متوجه تقلبی بودن آن ایمیل خواهند شد؛ چون آدرس ایمیل فرستنده یک آدرس مبهم و به اصطلاح پرت است که هیچ نزدیکی و قرابتی با ایمیل‌های ارسالی رسمی ندارد.

یکی دیگر از نکاتی که مردم می‌توانند به آن توجه کنند این است که اگر از طرف یک بانک یا دستگاه متولی برای‌شان پیامکی ارسال شد و در آن پیامک لینکی تعبیه شده بود، به هیچ‌وجه آن لینک را باز نکنند و برای بررسی و صحت‌سنجی اطلاعات ارسالی، خودشان از طریق وارد کردن آدرس آن بانک، به سایت مورد نظر وارد شوند.

البته باید اطلاع‌رسانی در حوزه فیشینگ از طریق رسانه‌های جمعی مانند صداوسیما و رسانه‌های دیگر برای مردم صورت گیرد تا سواد رسانه‌ای در این زمینه افزایش پیدا کند.