



پشت پرده آگهی‌های استخدام؛ سوءاستفاده و اخاذی از زنان در فضای مجازی

رئیس پلیس فتا تهران بزرگ درباره سوءاستفاده کلاهبرداران از آگهی‌های جعلی استخدام برای فریب و اخاذی از زنان هشدار داد.

به گزارش بازارکار، پرونده‌های فیشینگ و کلاهبرداری سایبری در سال‌های اخیر با تغییر شیوه‌های مجرمان، شکل‌های تازه‌ای پیدا کرده‌اند. مجرمان با سوءاستفاده از دغدغه‌ها و اخبار روز جامعه، پیام‌هایی را برای شهروندان ارسال می‌کنند که در ظاهر حاوی یک خدمت، اطلاعیه یا هشدار فوری است، اما در واقع کاربر را به سمت لینک یا فایل آلوده هدایت می‌کند.

در یکی از پرونده‌های مورد بررسی پلیس فتا تهران بزرگ، متهم در جریان بازجویی درباره شیوه فعالیت خود توضیح داده است که لینک‌های آلوده را متناسب با موضوعات روز طراحی و برای شهروندان ارسال می‌کرده است.

وی در پاسخ به پرسش بازپرس درباره شیوه کار خود گفت: لینک‌هایی با موضوعاتی مانند تصاویر قدیمی و ابزارهای هوش مصنوعی ارسال می‌کردیم و افرادی که از گوشی‌های اندرویدی استفاده می‌کردند، پس از نصب فایل، دسترسی‌هایی را در اختیار ما قرار می‌دادند.

این متهم افزود: پس از دسترسی به تلفن همراه قربانی، امکان مشاهده پیامک‌ها و در نتیجه دسترسی به پیامک‌های رمز یک‌بار مصرف فراهم می‌شد و از این طریق حساب بانکی قربانیان مورد سوءاستفاده قرار می‌گرفت.

سوءاستفاده از حساب پیام‌رسان قربانیان

در این پرونده، سوءاستفاده مجرمان تنها به برداشت از حساب‌های بانکی محدود نبوده است. متهم در جریان بازجویی از دسترسی به حساب پیام‌رسان برخی قربانیان و ارسال پیام برای دوستان و آشنایان آنها خبر داده است.

در یکی از موارد، قربانی پس از خروج ناگهانی از حساب پیام‌رسان خود متوجه شد فرد دیگری با استفاده از حساب او برای دوستان و آشنایانش پیام ارسال کرده و با ادعای گرفتار شدن و نیاز فوری به پول، از آنها درخواست واریز وجه کرده است.

بر اساس اظهارات مأمور پرونده، در این مورد متهم نتوانسته بود به دلیل قرار داشتن پیامک رمز بانکی روی تلفن دیگری، حساب بانکی قربانی را خالی کند و به همین دلیل از حساب پیام‌رسان وی برای فریب و اخاذی از اطرافیان استفاده کرده بود.

هوش مصنوعی؛ پوشش جدید مجرمان سایبری

سردار داوود معظمی گودرزی، رئیس پلیس فتا تهران بزرگ، با اشاره به تغییر مستمر شگردهای مجرمان سایبری اظهار کرد: مجرمان تلاش می‌کنند روش‌های خود را متناسب با فناوری‌های روز به‌روزرسانی کنند و یکی از شگردهای جدید، سوءاستفاده از عنوان «هوش مصنوعی» است.

وی افزود: پیش از این عناوینی مانند «یارانه معیشتی» یا «ثنا» برای هدایت کاربران به سمت لینک‌های آلوده مورد استفاده قرار می‌گرفت، اما اکنون ممکن است پیامی با این مضمون ارسال شود که «تصویر شما را با هوش مصنوعی تغییر دادم» و فایلی نیز همراه پیام قرار گیرد. رئیس پلیس فتا تهران بزرگ ادامه داد: این فایل‌ها ممکن است در قالب PDF یا فایل‌های اجرایی مانند APK ارسال شوند و کاربر با کلیک و نصب آنها، ناخواسته دسترسی‌هایی را به مجرم سایبری بدهد.

گودرزی هشدار داد: در چنین شرایطی مجرم می‌تواند به پیامک‌های تلفن همراه دسترسی پیدا کند، فرآیندهای احراز هویت پیامکی را دور بزند، وارد پیام‌رسان‌ها شود و خود را جای قربانی معرفی کند. در صورت دسترسی به پیامک‌های بانکی نیز امکان سوءاستفاده مالی وجود دارد. وی تأکید کرد: حتی اگر لینک یا فایل از سوی یکی از اعضای خانواده یا دوستان ارسال شده باشد، نباید بدون بررسی روی آن کلیک کرد؛

چراکه ممکن است حساب همان فرد هک شده باشد و پیام بدون اطلاع او ارسال شده باشد.

پیام‌های جعلی با چاشنی ترس و اضطراب

سرگرد محمدحسین متذکر، رئیس اداره مبارزه با جرائم سایبری پلیس فتا تهران بزرگ نیز درباره یکی از روش‌های رایج مجرمان گفت: این افراد معمولاً پیامک‌های متعددی را از سرشماره‌های مشخص و غیرمرتبط با نهادهای رسمی ارسال می‌کنند.

وی افزود: محتوای این پیام‌ها اغلب با ایجاد ترس و اضطراب طراحی می‌شود؛ برای مثال پیام‌هایی با مضمون حکم جلب شما صادر شده، مشمول پرداخت مالیات شده‌اید، یارانه معیشتی به شما تعلق گرفته یا پیام‌هایی که فرستنده خود را یکی از آشنایان مخاطب معرفی می‌کند.

متذکر ادامه داد: در مرحله بعد، کاربر برای مشاهده جزئیات یا دریافت خدمات به کلیک روی لینک و نصب یک نرم‌افزار هدایت می‌شود و با نصب بدافزار، مجوز دسترسی به بخش‌هایی از تلفن همراه خود را در اختیار مجرم قرار می‌دهد.

وی تأکید کرد: شهروندان نباید فایل‌های بانکی، ایمیل‌های جعلی یا لینک‌های ناشناس را در فضای مجازی باز کنند؛ زیرا مجرمان ممکن است از طریق بدافزار به صندوق پیامکی دسترسی پیدا کرده و رمزهای یک‌بار مصرف را مشاهده کنند.

هشدار درباره پیامک‌های جعلی با عنوان نهادهای رسمی

رئیس اداره مبارزه با جرائم سایبری پلیس فتا تهران بزرگ با اشاره به پیامک‌های منتسب به دستگاه‌های دولتی گفت: شهروندان باید نسبت به سرشماره‌های ناشناس و پیام‌هایی که همراه با لینک ارسال می‌شوند، حساس باشند.

وی افزود: برخی دستگاه‌ها و سامانه‌های رسمی از سرشماره‌های مشخص برای اطلاع‌رسانی استفاده می‌کنند و شهروندان باید پیام‌های جعلی را از پیام‌های رسمی تفکیک کنند.

متذکر همچنین بر خودداری از نصب نرم‌افزار از منابع نامعتبر تأکید کرد و گفت: اگر شهروندان به نرم‌افزاری نیاز دارند، باید آن را از منابع معتبر دریافت و نصب کنند.

اعتراف متهم به استفاده از دغدغه‌های روز مردم

متهم در ادامه بازجویی درباره نحوه انتخاب موضوع لینک‌ها اظهار کرد که ایده‌ها متناسب با مسائل روز جامعه انتخاب می‌شده است. وی در پاسخ به بازپرس که پرسید این موضوعات چگونه به ذهن آنها می‌رسید، گفت: افراد اصلی خارج از کشور بودند و ایده‌ها از سوی آنها مطرح می‌شد.

متهم افزود: در زمان پرداخت مالیات، موضوعات مالیاتی را مطرح می‌کردیم و در مقاطع دیگر از پرونده‌های قضایی و شکایت استفاده می‌کردیم؛ چون این موضوعات برای مردم همراه با ترس و اضطراب است و مجرمان از همین احساس برای وادار کردن افراد به کلیک روی لینک استفاده می‌کردند.

کارت‌های بانکی اجاره‌ای و جعل مدارک هویتی

در بخش دیگری از این پرونده، متهم درباره نحوه جابه‌جایی و نقد کردن وجوه حاصل از کلاهبرداری توضیح داد که تعداد زیادی کارت

بانکی اجاره‌ای در اختیار داشته است.

وی همچنین از جعل مدارک هویتی برای نقد کردن وجوه و خرید طلا خبر داد و گفت که در برخی موارد با استفاده از مدارک جعلی، مبالغ حاصل از کلاهبرداری را به طلا تبدیل می‌کردند و سپس آن را به فروش می‌رساندند.

بر اساس اظهارات مطرح‌شده در جریان بازجویی، در این پرونده تعداد قابل توجهی کارت بانکی وسیم‌کارت اجاره‌ای مورد استفاده قرار گرفته است.

اخاذی از قربانیان با آگهی‌های جعلی استخدام

یکی دیگر از بخش‌های قابل توجه پرونده، استفاده از آگهی‌های استخدامی برای جذب افراد و در اختیار گرفتن حساب‌های بانکی آنهاست. متهم درباره این بخش از فعالیت خود گفت که با انتشار آگهی‌هایی با عنوان‌هایی مانند «کار در منزل» و «استخدام فوری»، افراد را جذب می‌کرده و در برخی موارد پس از دریافت تصاویر خصوصی از قربانیان، از آنها برای تهدید و اخاذی استفاده می‌کرده است.

وی همچنین اعتراف کرد که از برخی تصاویر برای سوءاستفاده در فرآیندهای احراز هویت صرافی‌ها استفاده شده است.

مقصد پول‌های سرقت‌شده؛ یک زنجیره چندلایه

سردار گودرزی در تشریح مسیر انتقال وجوه حاصل از کلاهبرداری گفت: فرآیند انتقال پول در این پرونده‌ها معمولاً چندلایه است و مجرمان تلاش می‌کنند مسیر وجوه را پیچیده کنند.

وی افزود: در یکی از روش‌ها، مجرمان با انتشار آگهی استخدام دورکاری، از افراد می‌خواهند حساب بانکی باز کنند و همزمان در یک صرافی رمزارز حساب کاربری ایجاد کنند. سپس به آنها گفته می‌شود مبالغی که به حسابشان واریز می‌شود، عایدات یک شرکت بازرگانی است و باید آن را به رمزارز تبدیل کنند.

رئیس پلیس فتا تهران بزرگ هشدار داد: فردی که با این عنوان وارد چنین فرآیندی می‌شود ممکن است بدون اطلاع از ماهیت واقعی فعالیت، وارد چرخه جرم شود و وجوه متعلق به ده‌ها یا صدها نفر به حساب او منتقل شود؛ در نتیجه خودش نیز ممکن است تحت پیگرد قانونی قرار گیرد.

وقتی قربانی، بخشی از زنجیره جرم می‌شود

شهرام لرستانی، معاون دادستان و سرپرست دادسرای عمومی و انقلاب جرائم رایانه‌ای نیز با اشاره به گستردگی عناوین جرائم سایبری گفت: جرائم مالی مانند کلاهبرداری و سرقت در حقوق کیفری در زمره جرائم علیه اموال قرار می‌گیرند، اما آثار این جرائم تنها مالی نیست و می‌تواند امنیت و آرامش مردم را نیز تحت تأثیر قرار دهد.

وی با تأکید بر ضرورت حفظ آرامش هنگام دریافت پیام‌های مشکوک گفت: شهروندان نباید هنگام مواجهه با پیام‌هایی درباره پرونده قضایی، بسته پستی، وام، یارانه، امور مالیاتی یا مسائل مشابه دچار اضطراب شوند و بدون بررسی روی لینک کلیک کنند.

وی افزود: اصل را باید بر این گذاشت که لینک‌های ناشناس می‌توانند آلوده باشند و افراد باید پیش از هر اقدامی، صحت پیام و فرستنده آن را بررسی کنند.

اگر گوشی آلوده شد چه کنیم؟

سرگرد متذکر درباره اقدامات اولیه پس از آلوده شدن تلفن همراه گفت: نخستین اقدام، قطع ارتباط گوشی با شبکه است و کاربر می‌تواند دستگاه را در حالت پرواز قرار دهد.

وی ادامه داد: سپس باید در تنظیمات گوشی، نرم‌افزارهایی که به پیامک‌ها و سایر بخش‌های حساس دسترسی دارند بررسی شوند و مجوزهای غیرضروری لغو یا نرم‌افزار مشکوک حذف شود.

متذکر همچنین فعال‌سازی ورود دومرحله‌ای در پیام‌رسان‌ها را یکی از اقدامات مهم امنیتی دانست و بر رعایت اصول امنیتی در استفاده از تلفن همراه تأکید کرد.

پلیس فتا: شگرد مجرمان هر روز تغییر می‌کند

رئیس پلیس فتا تهران بزرگ با تأکید بر اینکه شگردهای مجرمان سایبری ثابت نمی‌ماند، گفت: ممکن است امروز پیام جعلی با عنوان هوش مصنوعی یا مالیات ارسال شود و فردا از موضوع دیگری که دغدغه روز مردم است برای فریب شهروندان استفاده شود.

وی از شهروندان خواست به پیام‌های حاوی لینک که از منابع ناشناس یا غیررسمی ارسال می‌شوند اعتماد نکنند و نرم‌افزارهای مورد نیاز خود را تنها از منابع معتبر دریافت کنند.

شهروندان در صورت مواجهه با موارد مشکوک یا وقوع کلاهبرداری سایبری می‌توانند با مرکز امداد و فوریت‌های سایبری پلیس فتا به شماره ۰۹۶۳۸۰