آیا از ترکیب دوربین قوی و شبکه‌های اجتماعی باید ترسید؟

کابوسی به نام ناامنی

صالح سپهری‌فر

چند روز پیش رسانه‌های ژاپنی، خبر ایجاد مزاحمت فردی برای یک هنرمند سرشناس این کشور را منتشر کردند. با این که شاید این خبر برای بسیاری از ما جذابیت خاصی نداشته باشد، اما شیوه‌ای که این فرد مزاحم توانست به نشانی محل سکونت این هنرمند سرشناس دست یابد، عجیب و در عین حال نگران‌کننده است. ماجرا از این قرار بود که این مرد ابتدا یکی از تصاویر این هنرمند در شبکه‌های اجتماعی را بررسی کرده و با اندکی دقت متوجه شد که می‌تواند باز تاب تصویر مکانی مشخص را در چشمان او شناسایی کند. این فرد مزاحم در گام بعدی توانست ایستگاه قطاری را که این هنرمند از خانه برای رفتن به محل کار استفاده می‌کند تشخیص دهد و سپس با استفاده از سامانه استریت ویوو گوگل (Street View) و نیز برخی جزئیات دیگر، خانه‌اش را شناسایی کند. هدف این مرد، ایجاد مزاحمت برای این هنرمند بود. با این که تردیدی در هوش بالای این مزاحم در استفاده از چنین شیوه‌ای وجود ندارد، اما بیایید به این ماجرا از زاویه‌ای دیگر نگاه کنیم.

نگرانی‌ها درباره حفظ حریم خصوصی

این اتفاق موجب ایجاد پرسش‌ها و نگرانی‌های متعددی در خصوص حریم خصوصی شد. واقعیت این است که امنیت کاربران در عصری که تصاویری باکیفیت بالا در شبکه‌های اجتماعی به اشتراک گذاشته می‌شود، به‌راحتی قابل حفاظت نیست. در واقع، تصاویر روزمره‌ای که ممکن است از طریق شبکه‌های اجتماعی با دیگران به اشتراک بگذاریم، ممکن است در نهایت مواردی را که می‌خواهیم از دیگران پنهان نگه داریم، فاش کند.

این روزها حتی یک گوشی متوسط هم می‌تواند تصاویری باکیفیت و جزئیات بالا را به ما بدهد. بسیاری از ما به شبکه‌های اجتماعی دسترسی داریم و به‌راحتی این تصاویر را در اختیار دیگران قرار می‌دهیم. شاید وقت آن شده بپذیریم استفاده از شبکه‌های اجتماعی می‌تواند چنین مخاطراتی نیز داشته باشد.

یک عادت؛ یک تهدید

افراد زیادی، لحظات مختلف زندگی خود را در شبکه‌های اجتماعی نظیر اینستاگرام با دیگران به اشتراک می‌گذارند. در این میان، برخی کاربران از جمله افراد سرشناس دنیای هنر یا ورزش، علاقه بیشتری به این کار دارند، زیرا نه تنها با این روش به تقویت برند شخصی خود کمک می‌کنند، بلکه حتی می‌توانند کسب درآمد هم داشته باشند.

از سویی دیگر، شرکت‌های پیشرو در زمینه تولید گوشی‌های هوشمند به‌شدت به رقابت با یکدیگر برای ارائه دوربین‌هایی بهتر به مشتریان مشغولند، به طوری که یکی از اصلی‌ترین شاخص‌های ارزیابی کیفیت یک گوشی جدید، قابلیت‌ها و مشخصات فنی دوربین آن است.

برای نمونه، گوشی جدید آیفون ۱۱ پرو دارای سه لنز در دوربین است و به‌زودی یک به‌روزرسانی نرم‌افزاری برای بهره‌گیری از هوش مصنوعی به منظور نمایش بهتر جزئیات نیز به آن افزوده می‌شود. گوشی گلکسی ای۹ سامسونگ نیز دوربینی سه لنزه دارد و گوشی معروف هوآوی با نام پی۳۰پرو هم از ترکیبی قدرتمند از سخت‌افزار و نرم‌افزار بهره می‌برد که امکان زوم ۵۰ برابری را فراهم می‌کند.

این میزان از دقت و جزئیات از یک سو و حجم بالای تصاویری که کاربران و به‌ویژه افراد سرشناس از خود در شبکه‌های اجتماعی ارسال می‌کنند، می‌تواند مشکلاتی را نظیر همان خواننده ژاپنی برایشان به همراه آورد.

به همین دلیل، معمولا به افراد معروف توصیه می‌شود مراقب باشند تصاویری این چنینی را با طرفداران خود به اشتراک نگذارند. خودداری از به‌اشتراک‌گذاری هر نوع اطلاعات زنده (نظیر پخش زنده از محلی که در آن حضور دارند)، خودداری از عکس گرفتن از محل زندگی و محله‌ای که در آن ساکن هستند، از جمله دیگر توصیه‌هایی است که به این افراد می‌شود. برخی کارشناسان می‌گویند در صورتی که فردی بیش از صد هزار دنبال‌کننده یافت، باید به‌شدت مراقب هر نوع نشانه قابل شناسایی در تصاویرش باشد.

البته سال‌هاست بسیاری از هنرپیشه‌ها و افراد معروف و پرطرفدار در حوزه‌های مختلف، یک سری تدابیر امنیتی را رعایت می‌کنند. با این وجود، امکان لو رفتن اطلاعات شخصی از طریق تصاویر به اشتراک‌گذاشته شده در شبکه‌های اجتماعی موضوع جدیدی است که شاید برخی آن را کم‌اهمیت بدانند.

در ماجرای هنرمند ژاپنی، گفتیم فرد مزاحم با استفاده از سامانه نقشه گوگل و قابلیت «استریت ویوو» که امکان مشاهده خیابان و خانه‌ها را به کاربر می‌دهد، توانست موقعیت دقیق منزل این هنرمند را شناسایی کند. این مساله سبب شد انگشت اتهام یک بار دیگر به سوی گوگل گرفته شود.

پیش از این نیز برخی کارشناسان درباره امکان سوءاستفاده از این سامانه هشدار داده بودند. جالب است بدانید برخی کشورها نظیر هند درخواست گوگل برای گنجاندن خیابان‌های این کشور در سامانه مذکور را به همین دلیل رد کرده‌اند. همچنین فشارهای وارده در ایالات متحده به گوگل سبب شده این شرکت در تصاویر خیابان‌ها در این سامانه، پلاک خودروها و نیز چهره افراد مشخص در تصاویر را بپوشاند. با این وجود، باز هم جزئیات دیگری نظیر حیوانات خانگی همراه افراد یا نقاشی‌های روی دیوار کاملا در این تصاویر به‌صورت واضح نمایش داده می‌شود.

داستانی که همچنان ادامه دارد

می‌گویند همراه با پیشرفت فناوری، شیوه‌های سوءاستفاده از آن هم پیشرفت می‌کند. شاید مواردی که دیدیم، تنها بخشی از سوءاستفاده‌هایی باشد که بتوان از تصاویر باکیفیت کاربران انجام داد. با وجود این‌که احتمالا هنوز راه‌های رفته و نرفته دیگری در این زمینه وجود دارد، شاید بهتر باشد با اندکی احتیاط، تا حد امکان جلوی بروز مشکلاتی این‌چنینی را بگیریم.

سلفی‌هایی که بلای جان می‌شود

امروزه استفاده از اثر انگشت برای باز کردن قفل گوشی‌های هوشمند، قفل‌های هوشمند محل کار یا منزل و احراز هویت در برخی مراکز، اقدامی عادی به شمار می‌رود. اثر انگشت یک قابلیت منحصربه‌فرد برای هر فردی است و به همین دلیل، امکان جعل و بازسازی آن دشوار است.

با این وجود، همین دوربین‌های قدرتمند تلفن همراه می‌تواند دردسری جدی در این زمینه ایجاد کند. مدتی پیش مطالعه‌ای از سوی پژوهشگران ژاپنی منتشر شد که نشان می‌داد با بررسی دقیق تصاویر سلفی یا معمولی که در آن فرد، دو انگشت خود را به نشانه پیروزی بالا گرفته می‌توان اثر انگشت او را بازسازی کرد.

اما دردسرهای دستیابی فردی تبهکار به اثر انگشت ما می‌تواند به‌مراتب بدتر از دستیابی به گذرواژه‌هایمان باشد. یک گذرواژه را می‌توان به راحتی تغییر داد، اما اثر انگشت این گونه نیست و امکان تغییر آن وجود ندارد.

با گسترش استفاده از فناوری احراز هویت با اثر انگشت و مجهز شدن دستگاه‌های بیشتری به آن، پیامدهای مخرب دسترسی غیرمجاز دیگران به اثر انگشت‌مان بسیار بیشتر از گذشته خواهد بود.

اگر مطالب این صفحه را می‌پسندید، عدد ۷۲۸۲ را به شماره ۳۰۰۰۱۱۲۲۶ پیامک کنید