سلفی‌های دردسرساز

مراقب باشید چه سلفی‌هایی در فضای مجازی منتشر می‌کنید

هکرها از طریق یک سلفی می‌توانند مکانی که یک فرد در آن حضور داشته را شناسایی کرده، سن یک فرد را به دست آورده و در نهایت اطلاعاتی که حتا یک فرد تصور آن‌را نمی‌کند را به دست آورند. سوال اصلی این است که این تصاویر چگونه به دست می‌آیند و مهم‌تر از آن با چه هدفی مورد استفاده قرار می‌گیرند؟

سلفی شما اطلاعات زیادی در ارتباط با شما بازگو می‌کند. سلفی گرفته شده در یک مراسم مکانی که یک فرد در آن قرار داشته است، ماهی که این سلفی گرفته شده، سن فردی که این سلفی را گرفته وانبوهی اطلاعات دیگر را بازگو می‌کند. انتشار این اطلاعات شما را به وحشت انداخته است؟ عجله نکنید این تنها بخش خوب داستان است. من یک سلفی برای یکی از دوستانم آپلود می‌کنم. این عکس با استفاده از یک آی‌فون 7 گرفته شده است. خورشید در پس‌زمینه عکس می‌درخشد. یک ردیف از درختان در امتداد رودخانه قرار دارند. به نظر می‌رسد، این‌گونه اطلاعات بی ضرر هستند و یک عکس با هدف ثبت یک لحظه و ارسال یک عکس یادگاری گرفته شده است. اما زمانی که این عکس را روی یک سایت آپلود می‌کنید به هکرها کمک کرده‌اید تا اطلاعاتی درباره شما به دست آورند. زمانی که عکسی گرفته می‌شود یکسری متادیتاها درون یک عکس ذخیره می‌شوند. اطلاعاتی که ممکن است در اختیار هکرها قرار بگیرد.

مطلب پیشنهادی

امپراطوری آسیب پذیر!

آیا قدرت و توانایی هکرها بی حد و مرز است؟

اگر یک سلفی در ارتباط با یک مراسم خاص همچون عروسی باشد و این سلفی در سایتی آپلود شود، ممکن است برچسب‌هایی همچون عروس و عروسی به یک تصویر اضافه شود، بدون آن‌که شما دخالتی در این زمینه داشته باشید. در ادامه چیزی شبیه به تبلیغات فیسبوک در قالب یک متن در بالای تصویر قرار می‌گیرند. سایت Selfie Reveal در همین ارتباط کار خود را آغاز کرده است. در این سایت یک نمونه مفهومی از یک بازی به نام Watch Dog2 آماده شده و نشان می‌دهد هکرها چگونه قادر هستند عکس‌های به ظاهر بی خطر را به دست آورده و از اطلاعات درون تصاویر استفاده کنند.

این احتمال وجود دارد که اطلاعات به مراتب خطرناک‌تری در مقایسه با افشای مکان ضبط یک سلفی در اختیار هکرها قرار گیرد.
برچسب‌هایی که سایت‌ها روی یک عکس قرار می‌دهند در ادامه به بخشی از بایگانی گسترده آن‌ها تبدیل می‌شوند. در چنین حالتی این تصاویر به شرکت‌های تبلیغاتی فروخته می‌شود. دیوید ماینور، کارشناس هک داده‌ها در این ارتباط به نویسنده سایت Inc گفته است: « سایت Selfie Reveal تنها یک ترفند بازاریابی نیست، اگرچه با هدف جلب توجه شما طراحی شده است. هکرهای واقعی قادر هستند داده‌ها را از درون تصاویر استخراج کرده و از این داده‌ها برای پیدا کردن اطلاعات بیشتری در ارتباط با شما استفاده می‌کنند.» داده‌های EXIF که درون یک تصویر قرار می‌گیرند، شامل زمان و مکان هستند. هکرها از روتین‌های هوش مصنوعی استفاده می‌کنند تا سن، (این‌کار از طریق مقایسه یک تصویر با کتابخانه‌ای از تصاویرانجام می‌شود.)، ویژگی‌های بصری چهره و جنسیت شما را به دست آورده و همچنین به داده‌های کاربردی دیگر دست پیدا کنند. اگر یک فرد عادی جامعه باشید این اطلاعات به شرکت‌های تبلیغاتی فروخته شوند. اگر فرد مشهوری باشید این اطلاعات به منظور اخاذی مورد استفاده قرار می‌گیرند. در همه موارد هکرها قادر هستند اطلاعات را به شیوه دقیقی تجزیه و استخراج کنند. ماینور گفته است: «شما سلفی گرفتن را با قرار دادن عکس خود در منابع رایج و در دسترسی همچون فیسبوک یا لینکدین آغاز می‌کنید. در ادامه هکرها قادر هستند با استفاده از ابزارهای تحلیل‌گر، کاوش عمیقی در یک تصویر انجام دهند.»

هوش مصنوعی قادر است اطلاعات درون پس‌زمینه تصاویر را نیز مورد تحلیل قرار دهد. تصویر درون یک عکس برای یک انسان ممکن است عادی باشد، اما هوش مصنوعی قادر است متن‌هایی که درون پس زمینه تصاویر پیدا می‌کند را به بهترین شکل تجزیه کرده و از این اطلاعات به منظور ردیابی یک فرد در شبکه‌های اجتماعی دیگر استفاده کند.

تاریخ انتشار:

05 دی 1395

نشانی منبع: https://www.shabakeh-mag.com/security/6086