دپارتمان ترویج اینشورتک

مرکز نوآفرینی بیمه و مالی پلنت

چگونه از تهدیدات مربوط به تقلب جلوگیری و با آن مبارزه کنیم؟

مبارزه با تقلب در عکس و فیلم برای ارزیابی ریسک و خسارت در بیمه

ریسک‌هایتان را بشناسید و بدانید که اکنون چه اقدامی انجام دهید

وحیده نورانی

دی ماه ۱۴۰۳

مقدمه

شکی وجود ندارد که آینده بازرسی‌های مربوط به رسیدگی به خسارات و پذیره‌نویسی، به شدت به سمت سلف‌سرویس خواهد رفت. همیشه در بسیاری از موقعیت‌ها نیاز به بازرسی‌های تخصصی وجود خواهد داشت، اما قطار توسعه، مدت‌هاست که ایستگاه را به سمت مشتریانی که خواستار گزینه‌های سلف‌سرویس برای گرفتن و ارسال شواهد دیجیتالی هستند، ترک کرده است. این کار باعث می‌شود دستاوردهای بزرگی در کارایی و تجربه مشتری حاصل شود، در حالی که امکان استقرار راهکارهای برآورد و مدیریت مبتنی بر هوش مصنوعی و یادگیری ماشین را باز می‌کند. بدیهی است که این یک امتیاز برای بیمه‌گران و بیمه‌گذاران است.

همچنین امکان دستکاری آن شواهد را از طریق ابزارهای قدرتمندی فراهم می‌کند که حتی برای مصرف‌کننده‌هایی که کمتر با فناوری آشنایی دارند، (اغلب به صورت رایگان) به آسانی در دسترس قرار می‌گیرند.

در حالی که برخی از شرکت‌های بیمه‌گر از برنامه‌های اثبات اختصاصی برای کنترل برخی از این ریسک‌ها استفاده می‌کنند، این رویکرد با خواسته‌های مشتری مطابقت ندارد. مصرف‌کنندگان نمی‌خواهند برنامه شما را دانلود یا از آن استفاده کنند. این مسئله، یک کشمکش مداوم برای بسیاری از صنایع از جمله بیمه بوده است. آنها ارسال پیامک را به چت اختصاصی ترجیح می دهند و به اشتراک‌گذاری عکس‌هایی که می گیرند را به استفاده از تجربه عکس درون‌برنامه‌ای ترجیح می‌دهند. این بدان معناست که ما نمی‌توانیم برای کاهش ریسک کلاهبرداری به اپلیکیشن‌های خود اعتماد کنیم. ما باید در مورد اطمینان از صحت شواهد دیجیتال، صرف نظر از منبع آن، بیشتر فکر کنیم. این امر به معنای استقرار نسل جدیدی از ابزارهای تشخیص در همه رسانه‌ها است تا به سرعت و بدون مشکل، از واقعی بودن چیزی که به آن نگاه می‌کنیم اطمینان حاصل شود.

بخش اول

قابلیت کاربرد عکس‌ها در بیمه

از لحاظ تاریخی، بازرسی از اموال فیزیکی و محیط‌های اطراف، بخشی از فرآیند بیمه بوده است. این بازرسی‌ها، بازرسی در محل توسط یک پذیره‌نویس یا نماینده آنها بود. به‌طور کلی، یک پرونده کتبی از بازرسی ایجاد و نگهداری می‌شود تا در صورت خسارت از آن استفاده شود. از دهه ۱۸۰۰، از عکس‌ها برای ثبت نتایج این بازرسی‌ها استفاده می‌شد.

در حالی که "شواهد" بازرسی یا خسارت بیمه معمولا به سطح مورد نیاز قوانین نمی‌رسد، مرسوم است که مدارک عکاسی به عنوان بخشی از مدارک خسارت بیمه گنجانده شود. از آنجایی که ممکن است دعاوی خسارت مورد مناقشه قرار گیرند و به دادگاه راه پیدا کنند، عکس‌ها ممکن است در واقع مشمول شرایط «اصالت و واقعی بودن» باشند.

تا قبل از ظهور عکاسی دیجیتال و استفاده گسترده از آن در بیمه، امکان تغییر عکس‌ها برای اهداف تقلبی، به صورت محدود وجود داشت. امروزه با گزینه‌های متعددی که برای ویرایش عکس‌ها و فیلم‌های دیجیتالی در دسترس است، برخی با قابلیت‌های هوش مصنوعی و ابزارهای بسیاری که به آسانی در دسترس عموم است، موضوع صحت عکس و رسانه برای اهداف بیمه به سطح جدیدی از اهمیت ارتقا یافته است.

شواهد قانونی

در حدود سال ۸۰ قبل از میلاد، سیسرو برای اولین بار خواستار مفهوم دقیق "شواهد" شد. به نظر می‌رسد سخنرانی سیسرو در Pro Archia Poeta که به اهمیت شهادت شفاهی می‌پردازد، بحثی ۱۵۰۰ ساله را آغاز کرده است که توسط لرد بالفور در سال ۱۷۵۴، هنگامی که او نیاز به شواهد مکتوب را توضیح داد، از سر گرفته شد.

«اما موازنه احتمالات مسلما در طرف دیگر است، زیرا شهادت مردی درستکار هر چند که با تشریفات یک سوگند مستحکم همراه باشد، همچنان در معرض نقص حافظه است؛ چون انسان موضوعات را از یاد می‌برد. مردان مستعد این هستند که به جای خود نظرات خود سوگیری‌هایشان را بیان کنند و بنابراین استدلال‌ها در بیشتر موارد به سمت دیگری برمی گردند؛...»

بخش دوم

ظهور تهدید تقلب در رسانه‌های دیجیتال

از طریق فرآیند تحول دیجیتال، بصنعت بیمه برای اتخاذ تصمیمات عملی در مورد وضعیت دارایی‌های بیمه‌شده، هم برای خسارت و هم برای پذیره‌نویسی، به طور فزاینده‌ای به رسانه‌های دیجیتال متکی شده است. این مدرن‌سازی صنعت، که از بسیاری جهات فرآیندهای بیمه را ساده‌سازی و مصرف‌کننده‌محور کرده است، شکل‌های جدیدی از کلاهبرداری رسانه‌های دیجیتال را نیز به وجود می‌آورد که بیمه‌گران باید از آن آگاه باشند.

این تهدید جدید تقلب توسط دو روند مهم تداوم یافته است:

- نیاز روزافزون و گسترش راهکارهای بیمه سلف‌سرویس
- ظهور ابزارهای پیشرفته هوش مصنوعی برای ویرایش تصاویر یا فیلم‌ها

بیایید چند دقیقه به بررسی هر دوی این روندها بپردازیم تا مفاهیم عمیق‌تر را بهتر درک کنیم:

شمشیر دولبه فرآیندهای بیمه سلف‌سرویس

وقتی تلفن‌های همراه قدرت دوربین‌های تحت شبکه را در اختیار توده مردم قرار دادند، مطمئنا بر صنعت بیمه تأثیر گذاشتند؛ صنعت بیمه‌ای که برای تعیین وضعیت دارایی‌های بیمه شده به عکس‌ها متکی است. با تخمین‌های بیش از یک تریلیون عکس که سالانه توسط کاربران تلفن همراه گرفته می‌شود و بهبودهای سالانه سریع کیفیت دوربین موبایل، طبیعی است که تلفن‌های همراه به یک دستگاه اصلی برای جمع‌آوری عکس‌های مورد نیاز بیمه تبدیل شده‌اند.

این نوسازی صنعت، که از بسیاری جهات فرآیندهای بیمه را ساده کرده است ... . شکل‌های جدیدی از تقلب را نیز ایجاد می‌کند که لازم است بیمه‌گران از آن آگاه باشند.

تکثیر تلفن‌های همراه، دلیلی کافی برای ایجاد اختلال در روند سنتی اعزام بازرسان برای عکس گرفتن از دارایی‌های شخصی یا تجاری است. کیفیت عکس رضایت‌بخش و راحتی بهبود یافته،

احراز اصالت مدارک عکاسی

آیا می‌دانستید؟

از دهه ۱۹۳۰، دادگاه‌ها برای اینکه عکس‌ها مدرک قابل قبولی باشند، باید توسط عکاس «تأیید اصالت» شوند. به عنوان مثال، یک قاضی از عکاس می‌پرسد که آیا این عکس توسط او گرفته شده است و آیا یک بازنمایی واقعی از موقعیت است.

با رایج شدن عکاسی دیجیتال، زنجیره جرم‌شناسی قضایی برای تجزیه و تحلیل عکس‌های دیجیتال اعمال شد.

اولین عکس دیجیتال در سال ۱۹۵۷ گرفته شد

از سال ۲۰۱۷، روش جدیدی برای اثبات قانونی اعتبار عکس توسط سیستم دادگاه اتخاذ شد. در آمریکا، قوانین فدرال مربوط به شواهد در ۱ دسامبر ۲۰۱۷ اصلاح و لازم‌الاجرا شد و احراز اصالت داده‌ها از منابع الکترونیکی (وب سایت، فایل از رایانه شخصی و غیره) را آسان‌تر کرد.

قوانین جدید نحوه احراز هویت سوابق "تولید شده توسط یک فرآیند یا سیستم الکترونیکی" را توصیف می کند. بر اساس این قوانین جدید، یک وکیل دیگر نیازی به شاهد یا کارشناس برای احراز هویت انواع خاصی از سوابق نخواهد داشت. اکنون، گواهی کتبی ارائه شده توسط شخصی با دانش فنی مربوطه مبنی بر معتبر بودن مدارک قابل قبول است، اما همچنان توسط طرف مقابل قابل اعتراض است. این قوانین همچنین امکان استفاده از «فرآیند شناسایی دیجیتال» (مانند مقادیر هش) را برای تأیید اعتبار داده‌های الکترونیکی آن چیزی که ادعا می‌شود، فراهم کردند.

یک علت قوی برای تبدیل بسیاری از خسارات و بازرسی‌ها به سلف سرویس است که در حال حاضر به صورت دستی توسط بازرسان انجام می‌شوند.

این تحول چندان جدید نبوده است. در واقع، جای تعجب نیست که دهه گذشته منجر به نفوذ برنامه‌های تلفن همراه در صنعت شده است که روند بازیابی عکس از مشتریان بیمه‌شده را نسبتا آسان کرده است.

همانطور که مشخص است، بسیاری از ارائه‌دهندگان بیمه قبلا فرآیندهای سلف‌سرویس را برای انواع خاصی از قیمت‌ها، خسارات، بازرسی‌ها و تمدیدها، برای بیمه اموال و حوادث اجرا کرده‌اند. با این حال، استقرار و پذیرش دقیقا در سراسر صنعت به صورت جهانی اتفاق نیفتاده است.

یکی از دلایل آن نگرانی در مورد تقلب است. اما چه کسی می‌تواند صنعتی را که با تقلبی که تقریبا ۱۰ درصد از پرداخت‌های خسارت را تشکیل می‌دهد، سرزنش کند که چرا از چنین سیستمی که به طور ضمنی برای گرفتن و ارسال عکس‌ها به مشتریان اعتماد می‌کند، استقبال نکرده است؟

بسیاری از بیمه‌گران مجبور هستند که بده بستان بین افزایش ریسک کلاهبرداری در مقابل هزینه نگهداری واسطه‌ها یا کارمندان مورد اعتماد برای عکس‌برداری را مد نظر داشته باشند.

در نظر بگیرید که اتکا به بیمه‌شده برای گرفتن عکس یا فیلم از دارایی بیمه‌شده چه اشکالی دارد. برای شروع، بیمه‌گر چگونه مطمئن می‌شود که عکس‌های ارسالی از مکان و زمان درستی هستند؟ بیمه‌گر چگونه می‌داند که عکس‌ها با دارایی مورد نظر مطابقت دارند؟

نامحتمل نیست که عکس‌ها به سادگی از اینترنت دانلود شده و خسارت جعلی باشد. در حالی که اکثر عکس‌های دیجیتال از برچسب‌گذاری زمان و مکان استفاده می‌کنند، اکنون بیمه‌گران باید این ویژگی‌ها را تایید کنند و احتمال تغییر آن‌ها را در نظر بگیرند.

از آنجایی که فراداده عکس و فیلم به روشی غیرقابل تغییر یا ضددستکاری پایدار نیست، تعیین اینکه دستکاری شده است یا نه، به تجزیه و تحلیل قابل توجهی برای هر عکس نیاز دارد و خسارات اغلب شامل عکس‌های متعددی می‌شوند.

با توجه به بده‌بستان در ریسک‌ها و پاداش‌های استراتژی‌های سلف‌سرویس، بیمه‌گران به دو دسته تقسیم می شوند:

- پذیرندگان سلف سرویس که اجتناب‌ناپذیری و ریسک سلف‌سرویس را پذیرفته و ریسک را در مدل‌های کسب‌وکار خود وارد می‌کنند.

- غیر پذیرندگانی که بازرسی دستی «شخص مورد اعتماد» از دارایی‌ها را ادامه می‌دهند تا از افزودن ریسک جدید به فرآیندی که از قبل مستعد تقلب است، جلوگیری کنند.

در حالی که پذیرندگان، سیستمی متکی به اعتماد و فاقد نظارت را انتخاب کرده‌اند که ریسک تقلب خاصی را اضافه می‌کند، ممکن است احساس کنند که این خطر با صرفه‌جویی در هزینه، راحتی و افزایش بالقوه در وفاداری مشتری در خدمات سلف‌سرویس جبران می‌شود.

پردازش مستقیم، که در آن یک مشتری بیمه‌شده می‌تواند فرم خسارتی را از خانه خود پر کند، عکس‌ها را ارسال کند و چک خسارت را به صورت خودکار دریافت کند، عامل بسیار قدرتمندی برای رضایت و وفاداری مشتری است.

با این حال، پذیرندگان باید توجه داشته باشند که با دسترسی مشتریان به ابزارهای جدید ساده‌تر و قدرتمندتر ویرایش عکس و فیلم، خطر تقلب در عکس و ویدیو با گذشت زمان افزایش می‌یابد، موضوعی که در بخش بعدی به آن خواهیم پرداخت.

جالب اینجاست که هیچ زمانی عوامل خارجی نیاز به سلف سرویس را به اندازه شیوع کووید-۱۹ در اوایل سال ۲۰۲۰ در اولویت قرار نداده‌اند. شروع ناگهانی الزامات فاصله‌گذاری اجتماعی در بسیاری از موارد، ادامه فرآیندها و بازرسی‌های حضوری را بسیار دشوار کرد.

بسیاری از بیمه‌گران، هنگامی که با انتخاب مواجهه با تعداد زیادی از درخواست‌های بازرسی فیزیکی یا برنامه‌های تسریع‌کننده برای گسترش قابلیت‌های سلف‌سرویس مواجه می‌شوند، این مورد دوم را تنها انتخاب می‌دانند.

"... عوامل خارجی هیچ زمانی سخت‌تر از شیوع کووید-۱۹ در اوایل سال ۲۰۲۰، نیاز به سلف سرویس را افزایش نداده است."

در آینده، ممکن است نیاز بیمه‌گران را برای انجام هر چه بیشتر تراکنش‌ها به صورت مجازی یا به روش سلف سرویس تقویت شده باشد. در آن زمان، یعنی هنگامی که این وضعیت به عنوان بخشی از "ترمال جدید" مجازی پذیرفته شد، واقعا هیچ بازگشتی وجود ندارد.

عکس‌ها و ویدیوهای دیپ فیک (جعل عمیق) و تقویت شده با هوش مصنوعی

عصر عکس‌های دیجیتال در سال ۱۹۵۷ آغاز شد. با ظهور نرم‌افزار ویرایش عکس در سال ۱۹۸۷، اعتبار و قابل اعتماد بودن عکس‌های دیجیتال به طور مشروع زیر سوال رفت. با وجود این، امروزه عکس‌های دیجیتال معمولا در بسیاری از تصمیمات تجاری استفاده می‌شوند، شاید به این امید که بتوان تغییرات آماتوری در عکس‌ها را به راحتی ریشه‌یابی کرد.

برای اینکه فکر نکنید که دیپ‌فیک مشکلی محدود به رسانه‌های اجتماعی است، در نظر بگیرید که آنها در حال ایجاد مسیر ورود به شرکت‌ها هستند.»

در اواخر سال ۲۰۱۸ و ۲۰۱۹، ابزارهای تقویت‌شده با هوش مصنوعی برای تغییر رسانه‌های دیجیتال شروع به ظهور کردند؛ مانند دیپ‌فیک‌ها، که می‌توانستند فایل‌های موجود را گرفته و آن‌ها را به روش‌هایی تغییر دهند که برای چشم انسان و بسیاری از ابزارهای تشخیص دستکاری مبتنی بر ماشین غیرقابل تشخیص باشد. با پیشرفت فناوری هوش مصنوعی، فرض بر این است که این دستکاری‌ها، با اجتناب از ردگیری قضایی که معمولا با رسانه‌هایی مرتبط هستند که با ابزارهای ابتدایی‌تر تغییر یا ویرایش شده‌اند، به‌طور کامل غیرقابل شناسایی می‌شوند.

در بستر رسانه‌های اجتماعی، ممکن است نمونه‌هایی را دیده باشید که چگونه ویدیوهای دیپ‌فیک می‌توانند پیام‌های اینفلوئنسرها، سیاستمداران و بازیگران را تحریف کنند. شاید جعل عمیق مارک زاکربرگ، جعل ضعیف نانسی پلوسی، یا اعتراف یک هنرمند برتر دیپ‌فیک مبنی بر خلق یک هیولا، مشکل ویدیوهای تغییر یافته را فراتر از یک دردسر و گرفتاری حرکت داده باشد. ویدیوهای تغییریافته نه تنها واقعی‌تر شده‌اند، بلکه ساخت آنها نیز آسان‌تر شده است.

مبادا فکر کنید که دیپ‌فیک مشکلی محدود به رسانه‌های اجتماعی است، بلکه باید توجه داشته باشید که آنها مسیری را برای ورود به شرکت ایجاد می‌کنند. یک نمونه صدای تولید شده با هوش مصنوعی بود که با صدای مدیرعامل یک شرکت انرژی مطابقت داشت که برای کلاهبرداری نزدیک به ۲۵۰۰۰۰ دلاری از یک شرکت بیمه استفاده شد. آیا این یک اتفاق یکباره بود یا شروع یک شکل فریبنده‌تر از فیشینگ؟ اتکای صنعت بیمه به عکس‌ها و ویدئوهای دیجیتال برای تصمیم‌گیری عملی، آن را به ویژه در برابر این حمله جدید امنیت سایبری جدید مستعد می‌کند.

در حالی که اکچوئرها ممکن است بتوانند تهدید کلاهبرداری در رسانه‌های دیجیتال را نیز به حساب آورند، پیشرفت‌های مداوم فناوری تغییر رسانه‌های دیجیتال را برای تقریبا هر کسی آسان‌تر از همیشه می کند. از آنجایی که دنیای رسانه‌های اجتماعی به سرعت به این نتیجه رسیده‌اند که دیپ فیک‌ها اساسا ضرب‌المثل قدیمی "دیدن، باور کردن است" را تغییر داده‌اند و عکس‌ها و ویدئوهای بیشتری هر روز زیر سوال می‌روند، شکی نیست که مشکل روزافزون رسانه های جعلی آماده شتاب گرفتن در صنعت بیمه است.

با توجه به ظهور سریع و شتاب متعاقب آن، ما به درستی می‌توانیم استدلال کنیم که تهدید کلاهبرداری در رسانه‌های دیجیتال یک هدف متحرک است که نمی‌توان آن را به دقت اندازه‌گیری کرد یا در مدل‌های ریسک بیمه‌ای موجود گنجاند، مگر اینکه اقداماتی برای کاهش یا توقف تهدید انجام شود.

این روند جعل رسانه‌ای، که بعید است به این زودی‌ها از بین برود، مستلزم نگاهی جدی به چگونگی کاهش خطر ورود رسانه‌های تغییر یافته به جریان کاری بیمه دیجیتال است. نادیده گرفتن تهدید می‌تواند قرار گرفتن در معرض کلاهبرداری را چند برابر کند و بر نسبت خسارت تاثیر منفی بگذارد.

در نهایت، اقدام خردمندانه این است که مدیران بیمه یک رویکرد سیستمی را در نظر بگیرند که تضمین کند عکس‌ها و فیلم‌ها معتبر و بدون دستکاری هستند.

بخش سوم

ریسک‌های اکوسیستم بیمه

«اعتماد کن اما صحت و سقم آن را بررسی کن» یک ضرب‌المثل قدیمی روسی بود که اغلب توسط رونالد ریگان، رئیس جمهور اسبق آمریکا در چارچوب بحث‌های خلع سلاح هسته‌ای با اتحاد جماهیر شوروی نقل می‌شد. بعدها، جان کری، وزیر امور خارجه آمریکا گفت: ضرب‌المثل قدیمی پرزیدنت ریگان درباره «اعتماد کن، اما صحت و سقم آن را بررسی کن» نیازمند به‌روزرسانی است و ما در اینجا به استانداردی متعهد شده‌ایم که می‌گوید «صحت و سقم آن را بررسی کن و صحت و سقم آن را بررسی کن».

یکی از جنبه های قابل توجه اکوسیستم بیمه، تعداد ذینفعانی است که ممکن است در هر تراکنش خاصی دخیل باشند. به جز مشتری بیمه‌شده و بیمه‌گر، اغلب ممکن است در مورد خسارتی که شامل چندین بیمه‌شده باشد، بیمه‌گر دوم یا سوم وجود داشته باشند. برخی از مشتریان ممکن است از طریق نمایندگان یا کارگزاران کار کنند. شرکت‌های بیمه‌گر ممکن است ارزیابانی را برای ارزیابی خسارات بفرستند. این افراد اغلب ارزیابان مستقلی هستند که کارمندان مستقیم شرکت‌های بیمه نمی‌باشند. ادارات پلیس و آتش‌نشانی می‌توانند در رسیدگی به خسارات بیمه‌ای نقش اساسی داشته باشند. در نهایت، تعمیرگاه‌ها برای اطمینان از اینکه آسیب‌ها به طور کامل و درست تعمیر می‌شوند، بسیار مهم هستند تا ریسک‌های جدیدی در آینده ایجاد نشود.

هر یک از ذینفعان ممکن است در حال جمع‌آوری یا نگهداری اطلاعات مهم در رابطه با یک تراکنش بیمه‌ای، اغلب به شکل رسانه‌های دیجیتالی باشند که وضعیت دارایی بیمه‌شده را نشان می‌دهد. حفظ اعتماد به دقیق بودن دارایی‌ها در کل این اکوسیستم ذینفعان کار کوچکی نیست، به ویژه با درک این موضوع که تقلب می‌تواند از هر ذینفعی سرچشمه بگیرد.

عکس‌های دیجیتال در تصمیم‌گیری‌های بیمه‌ای دارای جایگاهی هستند، اما به شرط آن که بتوانیم به آن‌ها «اعتماد کنیم و صحت و سقم آن را بررسی کنیم» یا بهتر از آن، «صحت و سقم آن را بررسی کنیم و صحت و سقم آن را بررسی کنیم». در حالی که همه این ضرب‌المثل قدیمی را می‌دانند که «یک عکس می‌تواند به اندازه هزار کلمه ارزش داشته باشد»، یک تصویر دیجیتالی تغییریافته می‌تواند منجر به هزاران دلار خسارت تقلبی برای خسارت بیمه شود. در اکوسیستم پیچیده بیمه، نه تنها تشخیص تقلب ممکن است دشوار باشد، بلکه منشأ آن را نیز به سختی می‌توان مشخص کرد.

بخش چهارم

اقدام فوری

در حالی که در برخی از صنایع ممکن است توصیه شود که مراقب باشید و متوجه شوید که تهدید دستکاری رسانه‌های دیجیتال چگونه توسعه می‌یابد، در صنعتی که قبلا با سالانه میلیاردها دلار هزینه تقلب دچار مشکل شده است، اتخاذ رویکرد پیشگیرانه‌تری مطلوب است.

راه‌های زیادی را در نظر بگیرید که رسانه‌های متقلب، نادرست یا گمشده می‌توانند وارد معاملات بیمه شوند:

- عکس‌های قدیمی که ممکن است زمان یا تاریخ آنها دستکاری شده باشد.
- عکس‌هایی از آسیب اموال که در مکان دیگری گرفته شده باشند.
- عکس‌های موجود دانلود شده از اینترنت که برای پذیره‌نویسی یا خسارات استفاده می‌شوند.
- عکسی که ازعکس دیگری گرفته شده باشد یا عکس از صفحه نمایش.
- عکس‌ها/ فیلم‌های تغییریافته خسارت که برای اغراق در میزان خسارت استفاده می‌شود.
- عکس‌ها/ فیلم‌های تغییر یافته از کار تعمیر، که در واقع کار تعمیر به درستی تکمیل یا اصلا انجام نشده است.
- خسارت قبلی دارایی بیمه‌شده که هرگز ثبت نشده است.

در حالی که اینها تنها چند احتمال هستند که تقلب بالقوه را نشان می‌دهند، هر یک از این موارد از آسیب‌پذیری ذاتی پذیرش فیلم و عکس به طور مستقیم از مشتریان بیمه‌شده یا طرف‌های خارجی حکایت دارند. در حالی که برخی از این سوءاستفاده‌ها به مهارت فنی نیاز دارند، برخی دیگر را می‌توان با روش‌های ابتدایی مانند گرفتن عکس از مکان اشتباه انجام داد. در نهایت، باز کردن یک ویرایشگر عکس برای ویرایش عکس‌های دیجیتال، در عصر حاضر بازی کودکانه‌ای محسوب می‌شود.

به عنوان یک عامل پیچیده، تا زمانی که اقداماتی برای ردیابی وجود رسانه‌های دیجیتال دستکاری شده در معاملات بیمه انجام نشود، اندازه‌گیری اکسپوژر آن بسیار دشوار است. در موردی که کلاهبرداری پنهانی باشد، غفلت قطعا موجب خوشحالی نخواهد بود.

یک استراتژی معقول برای کاهش، با پذیرش تهدید رسانه‌های جعلی شروع می شود. همانطور که قبلا ذکر شد، این تهدید فقط در حال بدتر شدن است، به دلیل:

- بهبود و دسترسی آسان‌تر به فناوری تولید جعلی
- اتکای فزاینده به سلف‌سرویس در اکوسیستم پیچیده‌ای از ذینفعان با سطوح مختلف اعتماد

در حالی که تهدید کلاهبرداری رسانه‌ای خبر خوشی نیست، اما برای کسانی که اقدامی انجام دهند، امیدی وجود دارد. رهبران بیمه و فناوری اطلاعات، که در حال حاضر تمهیداتی را برای جلوگیری از رسانه‌های جعلی ایجاد می‌کنند، می‌توانند یک بنیان دیجیتالی امن ایجاد کنند که در آینده در برابر این تهدید مقاوم باشد و با این کار می‌توانند از قربانی شدن سازمان‌های خود جلوگیری کنند. در بخش‌های آینده، تعدادی از رویکردها را برای جلوگیری از موج تقلب رسانه‌ای بررسی می‌کنیم.

بخش پنجم

راه‌های مقابله با تقلب در عکس و فیلم

جلوگیری

راه‌هایی برای جلوگیری از تقلب در عکس و ویدیو وجود دارد، گرچه عموما ماهیت ساده‌ای دارند. کلاهبرداری بیمه‌ای، به هر حال یک جرم است، اما این موضوع به تنهایی به عنوان یک عامل بازدارنده برای میزان تقلب نرمی که صنعت بیمه سالانه تجربه می کند، عمل نکرده است.

روش‌های اجرایی فعلی برای شرکت‌های بیمه می‌تواند گران و زمان‌بر باشد. این روش‌ها ناکارآمد هستند و همیشه رعایت نمی‌شوند. به عنوان یک موضوع عملی، یک شرکت بیمه نمی‌تواند وارد کار اجرای قانون شود.

جریمه‌هایی که برای کسانی که به دنبال کلاهبرداری از شرکت‌های بیمه هستند اغلب:

- برای متعادل کردن "پاداش" کلاهبردار ناکافی هستند.
- تاخیر زمانی دارند.
- ارزش وقت و تلاش برای پیگرد قانونی ندارند.

در نتیجه، جلوگیری از تقلب اغلب به تهدید تعقیب کیفری تبدیل می شود. اینکه بیمه‌شده مجازات‌های مرتبط با کلاهبرداری را درک کند و با امضای خود تأیید کند که مرتکب کلاهبرداری نمی‌شود، یک اقدام متقابل معقول برای زیرمجموعه‌ای از جمعیت است. با این حال، به هیچ وجه راهی برای اطمینان از رعایت گسترده آن نیست.

و مهم‌تر از آن اینکه زیرمجموعه‌ای که این اقدامات متقابل روی آن‌ها جواب می‌دهد، آنهایی نیستند که عمدا مرتکب تقلب می‌شوند.

در سراسر اکوسیستم بیمه، دستیابی به یک استراتژی جامع‌تر پیشگیری از تقلب ممکن است نیاز به یک سیستم انگیزشی داشته باشد که امروزه بین ذینفعان متعدد آن که شامل موارد زیر هستند، وجود ندارد:

- کارکنان
- پیمانکاران یا ارائه‌دهندگان خدمات بلندمدت
- پیمانکاران یا ارائه‌دهندگان خدمات یکبار مصرف
- بیمه‌شده
- نمایندگان و کارگزاران
- قانونگذاران
- کارکنان دولت

یک اکوسیستم پیچیده و فقدان انگیزه و نیز تبانی احتمالی بین ذینفعان، جلوگیری را به ابزاری ضعیف برای ممانعت از تقلب در رسانه‌های دیجیتال تبدیل می‌کند.

تحلیل جرم‌شناسی

همانطور که قبلا ذکر شد، دنیای مدرن پر از تصاویر و ویدئوهای دیجیتال جعلی شده است. لباس می‌فروشند، ماشین می‌فروشند، نان ساندویچ و غیره می‌فروشند. آنها برای سرگرم کردن، عصبانی کردن یا هیجان زده کردن داستان می‌گویند. آنها می‌توانند سرگرم‌کننده باشند: تصاویری از شکلی که ما می‌خواهیم جهان آنگونه باشد، با تاری‌ها، فوکوس ملایم و هایلایت‌های دلنواز. آنها می‌توانند دراماتیک باشند: آفتاب درخشان روی یک زوج ژست‌گرفته که روی یک منظره سنگی نشسته‌اند.

اما ویدئوهای جعلی و مخرب؛ آنها می‌توانند به جای ارائه کمی ایده‌آل‌سازی جهان، دنیا را آنطور که نیست به ما نشان دهند. یک افسر شوروی پس از بی‌اعتنایی از کنار استالین حذف شد. انباری پر از صندوق‌های رای که هرگز آنجا نبوده‌اند، حادثه‌ای که اتفاق نیفتاده، تعمیراتی که هرگز انجام نشده و خسارت ناشی از آبی که هرگز رخ نداد.

جعلیات در اطراف همه ما وجود دارند. امواج جزر و مدی از تصاویر ایجادشده توسط هر کسی که دوربین و تلفن دارد بی‌وقفه بر چشمان ما می‌زند و ما را مات و مبهوت می‌کند. برخی از افراد با نادیده گرفتن دهه‌ها پیشرفت باورنکردنی در دستکاری رسانه‌ها، مطمئن هستند که می‌توانند تشخیص دهند چه چیزی واقعی است و چه چیزی جعلی.

برخی دیگر تسلیم می‌شوند و راه آسان را انتخاب می‌کنند: هر چیزی که می‌خواهند باور کنند که درست است، باید درست باشد و هر چیزی که باور نمی‌کنند، نباید درست باشد. برخی فقط امکان فریب را به عنوان هزینه زندگی در دنیای مدرن می‌پذیرند و تمام تلاش خود را می‌کنند تا این هزینه را در نظر بگیرند. بدیهی است که هیچ یک از اینها یک استراتژی قابل دوام برای عملیات حیاتی کسب‌وکار یا مأموریت حیاتی آن نیستند.

اما یک راه بهتر وجود دارد. با پیشرفت جعل‌کنندگان، کارآگاهان نیز بهبود پیدا کردند. جرم‌شناسی رسانه‌های دیجیتال، علم تجزیه و تحلیل تصاویر، ویدئو و صدا برای تشخیص دستکاری و جعل است. ممکن است مهم نباشد که بدانید برخی از اینفلوئنسرهای اینستاگرام از یک برس شفابخش برای از بین بردن لکه از روی پوست خود استفاده می‌کنند، اما مطمئنا وقتی عکس‌های خبری، فیلم‌های امنیتی یا عکس‌های صحنه جرم تغییر کرده باشند، این موضوع بسیار اهمیت دارد.

دو رویکرد کلی برای جرم‌شناسی رسانه وجود دارد: منفعل و فعال. تشخیص غیرفعال جعل (که به آن تشخیص کور نیز می‌گویند) یک رویکرد پس از واقعیت است که عکس‌ها و فیلم‌ها را برای تشخیص آثار به جا مانده از تغییرات تجزیه و تحلیل می‌کند، در حالی که تشخیص جعل فعال از تعدادی تکنیک مختلف استفاده می‌کند تا اطمینان حاصل شود که هرگونه تغییر ایجاد شده نمی‌تواند پنهان شود.

تشخیص فعال

از بین این دو رویکرد، تشخیص فعال آسان‌تر است. قرن‌هاست که مردم از آن استفاده می‌کنند. پادشاهان پاکت را مهر و موم می‌کردند و با نماد منحصر به فرد خود مهر می‌زدند. قفل نامه‌های الیزابتی امکان باز کردن مکاتبات را بدون پاره شدن غیرممکن می کرد، بنابراین هرگونه تلاش برای دستکاری آشکار می‌شد. اسکناس دلار آمریکا یک شاهکار واترمارکینگ است که شواهد اصلی آن به معنای واقعی کلمه در الیاف آن تعبیه شده است.

اما اقدامات فعال محدود هستند. برای اینکه این اقدامات مفید باشند، باید از همان ابتدا مستقر شوند. در واقع آن‌ها از دستکاری جلوگیری نمی‌کنند، بلکه فقط آن را آشکارتر می‌کنند. اگر کسی حوصله بررسی منشاء را نداشته باشد، می‌توان تصویری را که به‌طور فعال محافظت می‌شود، گرفت، دستکاری کرد و به‌عنوان واقعی نشان داد، درست مانند نامه‌ای روی سربرگ شرکت که اگر کسی زحمت بررسی امضا را نداشته باشد، می‌تواند به عنوان نامه واقعی منتشر شود.

با این حال، اگر تصاویر در هر نقطه تماسی تایید شوند، هر زمان که یک ذینفع آنها را مشاهده کند، اقدامات فعال می‌تواند به‌طور مؤثری به عنوان عامل ضددستکاری عمل کنند. علاوه بر این، شواهد ممیزی می‌تواند نشان دهد که در کجا ممکن است هرگونه دستکاری رخ داده باشد. لازمه این کار، پذیرش یکپارچه روش شناسایی و اعتبارسنجی فعال است.

تشخیص غیرفعال

تشخیص غیرفعال در سطح کاملا متفاوتی کار می‌کند. یک عکس معین، گاهی اوقات ممکن است که جزئیات سطح جعل را نشان دهد: یک سایه نامناسب، یک دست اضافی، یا تفاوت واضح در رنگ‌ها. اما در اغلب موارد، جعل باکیفیت هیچ نقصی ندارد که بلافاصله قابل درک باشد. بنابراین بسیاری از تکنیک‌های تشخیص غیرفعال جرم‌شناسی به جزییات نامحسوس تکیه می‌کنند؛ جزئیاتی که با «حذف تصویر از تصویر» باقی می‌مانند.

مسلما این عبارت گیج‌کننده‌ای است، اما روزهایی که فیلم عکاسی وجود داشت را در نظر بگیرید. عکاسان باتجربه اغلب می توانستند به عکس نگاه کنند و برند و نوع فیلم مورد استفاده، کاغذی که روی آن چاپ شده و حتی گاهی اوقات لنزی که عکس با آن گرفته شده را تعیین کنند. فیلم‌های مختلف، رنگ‌دانه‌های متمایز و واکنش‌های رنگی متفاوتی داشتند. کاغذهای مختلف دارای بافت‌های متمایز و خواص بازتابی بودند. لنزهای مختلف انحرافات رنگی خاص خود را داشتند که برای چشمی که به خوبی آموزش دیده قابل شناسایی است. همه این ویژگی‌ها با هم جمع می‌شوند تا نوعی ردیابی جرم‌شناسی را ارائه دهند که نه محتوای عکس، بلکه تاریخچه مختصری از نحوه ساخت آن را نشان می‌دهد.

در حالی که دقت عمل عکس‌های دیجیتالی بسیار بیشتر و مسلما واقعی‌تر است، ویژگی‌های ظریفی مانند نویز الکترونیکی گرفته شده در کنار فوتون‌ها،

معادل مدرنی برای رنگدانه‌های فیلم است. ممکن است کسی نتواند آن نویز را ببیند، اما نویز وجود دارد و یک الگوریتم جرم‌شناسی خوب ممکن است بتواند نه تنها برند، بلکه مدل دوربینی را که عکس را گرفته است، حتی در غیاب هر گونه اطلاعات دیگری شناسایی کند.

و کار به همین جا ختم نمی‌شود: هر تغییری که در یک تصویر ایجاد می‌شود، مصنوعات آماری ظریف خود را معرفی می‌کند. چرخش‌ها، تغییر اندازه‌ها، برش‌ها، اتصالات، فشرده‌سازی‌ها و غیره، همگی علائم خاص و جزئی خود را بر روی پیکسل‌ها در یک تصویر به جا می‌گذارند. اگر کسی تصویر را "سیگنال + نویز" در نظر بگیرد، تکنیک‌های غیرفعال جرم‌شناسی، برای بررسی نویز، سیگنال را از بین می‌برند.

تشخیص غیرفعال، مشابه تشخیص فعال، نیازی به پذیرش انتها به انتها ندارد و صرفا می‌تواند با دریافت تصویر توسط ذینفع نهایی انجام شود. این نوع تشخیص با اینکه سودمند است، ممکن است تا به حال حدس زده باشید که می‌تواند پیچیده هم باشد و اغلب به چندین الگوریتم جرم‌شناسی و هوش مصنوعی برای ریشه کن کردن جعلیات نیاز دارد. از آنجایی که پیچیدگی تولید تصویر، ناشناخته است، به طور کلی کمتر قابل اعتماد است و منفی‌های کاذب یا مثبت کاذب بیشتری نسبت به تشخیص فعال تولید می‌کند.

در مورد بیمه، سطح اطمینان اغلب بهترین چیزی است که می‌توان از شناسایی غیرفعال به دست آورد و اتخاذ تصمیم را به بیمه‌گر واگذار می‌کند تا مراحل بعدی را در مورد یک تصویر تقلبی بالقوه تعیین کند. اگر اندازه‌گیری غیرفعال، مثلا ۷۵ درصد اطمینان به صحت یک تصویر را گزارش کند، چگونه تصمیم می‌گیرید که آن تصویر واقعی است یا خیر؟ از دیدگاه انسان‌ها، قطعا باید این واقعیت را در نظر بگیریم که انسان‌ها در درک شهودی احتمالات و سطح اطمینان‌ها به طرز ناامیدکننده‌ای بد هستند.

سانسور در اتحاد جماهیر شوروی

نیکولای یژوف بعدا از این عکس حذف شد

نیکولای یژوف، تصویر سمت راست استالین، در کانال مسکو

باید عواملی مانند "تأثیر این باور که این عکس تغییر کرده است" را در نظر گرفت؟ آیا ممکن است متهم کردن مشتری به جعل، او را خشمگین کند؟ «اثر باور به صحت این عکس چه خواهد بود؟» آیا اگر تصویر واقعا به عنوان بخشی از یک طرح کلاهبرداری تهیه شود، منجر به خسارت به کسب‌وکار می‌شود؟

در نهایت، در حالی که نتایج با اطمینان بالا ممکن است قابل اقدام باشند، نتایج با اطمینان متوسط و پایین بعید است که هیچ اقدامی را تضمین کند، مگر اینکه عوامل دیگری وجود داشته باشند که وجود تقلب را تایید کنند.

مزایا و معایب و مقایسه راهکارهای مختلف

سه رویکرد جلوگیری، تشخیص منفعل و تشخیص فعال مانعه‌الجمع نیستند. در بیشتر موارد، جلوگیری نسبتا ارزان است، اگرچه تا حدودی بی‌اثر است ولی باید تا حد امکان استفاده شود. از سوی دیگر، تشخیص می‌تواند به مهار موج رو به رشد پیچیدگی عکس و ویدئوها کمک کند و توصیه می‌کنیم مناسب‌ترین اقدامات برای شرکت در نظر گرفته شود.

درست است که وجود یک تکنیک تشخیص فعال مانند انگشت‌نگاری یا واترمارکینگ در عکس دیجیتال به طور دقیق پاسخ می‌دهد که آیا این عکس تغییر یافته است یا خیر، اما این نیز درست است که تکنیک‌های فعال شکننده بوده و اغلب آنقدر به ساختارهای عمیق داده‌ها وابسته هستند که شکستن تصادفی آنها بسیار آسان است. حتی عمل ساده بیرون کشیدن یک قطعه از عکس یا فیلم دیجیتال می‌تواند به طور ناخواسته باعث تغییر اندازه یا فشرده‌سازی آن شود که اقدامات فعال را بی‌اعتبار می‌کند.

در نتیجه، تکنیک‌های فعال زیاد و راه‌های بی‌شماری برای قوی‌تر کردن آن‌ها وجود دارد. یک تکنیک فعال قوی، تکنیکی است که می‌تواند انواع تغییرات معمولی و نادیده‌ای که در طول چرخه زندگی یک قطعه عکس یا ویدئوی دیجیتال رخ می‌دهند و طوری عمل می‌کنند که عکس همچنان بدون تغییر شناخته شود، تشخیص دهد.

اما یک نکته وجود دارد: هنگامی که از ساختارهای سفت و سخت و شکننده فراتر رفتید و وارد ساختارهای مستحکم شدید، شروع به از دست دادن اطمینان خواهید کرد. دیگر نمی‌توانید با اقتدار مطلق بگویید "این عکس بدون تغییر است" یا "این عکس تغییر یافته است". در عوض، سطحی از اطمینان و باور به واقعیت آن تصویر برای شما فراهم می‌شود و هر چه تغییرات چرخه زندگی عکس شدیدتر باشند، سطح اطمینان کمتری خواهید

داشت. ممکن است توجه داشته باشید که این شبیه به نتایج گزارش‌های تشخیص غیرفعال است، با احتمالا آستانه خاصی از اقدام تضمین‌کننده اطمینان.

با این حال، بزرگترین مشکل در مورد اقدامات فعال شناسایی جعل این است که اکثر رسانه‌ها از آنها استفاده نمی‌کنند. یک عکس از تلفن شما تعداد زیادی متادیتا را حفظ می‌کند، اما به طور خودکار اثر انگشت‌دار، واترمارک یا ثبت نمی‌شود. دوربین فیلمبرداری هم بهتر از این عمل نمی‌کند. برای استقرار یک سنجش فعال نیاز به یک نرم‌افزار یا سخت‌افزار تخصصی است و عموما فقط افراد حرفه‌ای از آنها استفاده می‌کنند که اغلب عمدتا برای نگرانی‌های مربوط به کپی رایت است. اقدامات غیرفعال در اینجا وارد عمل می‌شوند و به عنوان مثال، به اقدامات فعال اجازه می‌دهند تا پس از عمل به کار گرفته شوند، البته از طریق شروع با اطمینان کمتر.

تکنیک‌های تشخیص غیرفعال در نهایت می‌توانند به عنوان مکملی برای ارائه درجه بالاتری از امنیت نسبت به تکنیک‌های فعال به تنهایی استفاده شوند. به طور مشابه، آنها را می توان به تنهایی مورد استفاده قرار داد، زیرا نصب آنها در یک نقطه پایانی، مانند ذخیره‌گاه تصویر آسان است، بدون اینکه نیازی به افزوده شدن آن به عنوان یک راهکار انتها به انتها به فرایندهای موجود باشد.

اگرچه آنها با اطمینان‌ها و باورها نیز سروکار دارند، اما می‌توانند فراتر رفته و مناطق مشکوک را مشخص کنند و حتی انواع تغییراتی که ممکن است ایجاد شده باشند را توصیف کنند. با توجه به یک قطعه فیلم یا عکس دیجیتالی که فعالانه از آن دفاع می‌شود و نمی‌تواند آستانه اطمینان را برآورده کند، اقدامات غیرفعال می‌تواند مکان و نحوه تغییر آن رسانه را مشخص کرده و به قضاوت انسان اجازه دهد تا کار کند. عقل سلیم آگاه تا حد زیادی کارگشاست و افراد را به سمت تصمیم گیری خوب می‌برد.

جدول صفحه بعد، مقایسه‌ای از اقدامات فعال و غیرفعال برای کشف تقلب در عکس و ویدئو را ارائه می‌دهد. اگرچه این جدول به هیچ وجه یک تحلیل کامل نیست، اما می‌تواند به عنوان نقطه شروعی برای تصمیم‌گیری در مورد نحوه مقابله با تهدید فزاینده عکس‌ها و ویدئوهای جعلی باشد.

در مجموع، مطمئن‌ترین راه برای اثبات اصالت رسانه‌های دیجیتال، یک فرآیند فعال بسیار امن است که در نقطه ضبط آغاز می‌شود و به دنبال آن یک فرآیند مدیریت چرخه حیات دقیق وجود دارد. با این حال، هنگامی که از آن مسیر خارج می شوید، اقدامات فعال قوی می‌تواند به طور یکپارچه در یک طرح تشخیص غیرفعال ادغام شوند تا تصمیمات بهتر، مفیدتر و مطمئن‌تری را ارائه دهند.

به خاطر داشته باشید که پارامترهای مختلف دیگری مانند تلاش برای یکپارچه‌سازی، الزامات اکوسیستم و هزینه کلی راهکار مورد استفاده برای هر دارایی، وجود دارند که می‌توانند تعیین کنند چه رویکردی برای شما بهتر است.

تکنیک تشخیص	اقدام برای یکپارچه‌سازی	الزامات اکوسیستم	اطمینان	تایید تغییرات چرخه زندگی	هزینه تشخیص برای هر دارایی
فعال	اضافه شدن به فرایندهای موجود	نیاز به پذیرش	بالا	خیر	کم
فعال مستحکم	اضافه شدن به فرایندهای موجود	نیاز به پذیرش	متغیر – بالا	بله	کم– متوسط
منفعل	بسیار کم یا هیچ	بدون الزامات	متغیر	محتمل	زیاد

بخش ششم

نتیجه‌گیری

بیمه ابزاری حیاتی و پیچیده است و از تمام جنبه‌های زندگی ما محافظت می‌کند و همانطور که بحث کردیم، به طور فزاینده‌ای در برابر روش‌های جدید تقلب و فریب آسیب‌پذیر است. با پذیرش رو به رشد سلف‌سرویس مشتری و روش‌هایی که از طریق آنها رسانه‌های دیجیتال می‌توانند به راحتی به خطر بیفتند، شروع اقدام برای به چالش کشیدن وضعیت موجود در پیشگیری از تقلب بسیار مهم است.

اقداماتی که امروز برای محافظت از کسب‌وکار خود انجام می‌دهید در سال‌های آینده به ثمر خواهند نشست. اکنون زمان پذیرش نوآوری و فناوری است که با پیشگیری و تشخیص پیشرفته کلاهبرداری، از کسب‌وکار بیمه محافظت کرده و آن را رشد می‌دهد.**

** این گزارش ترجمه Combat Digital Photo And Media Fraud In Insurance از **Attestiv Inc.** است.