فناوری‌های مالی

فصلنامه تخصصی کاربرد نوآورانه فناوری در ارائه خدمات مالی

شماره ۱

تابستان ۱۴۰۱

پرونده این شماره:

کشف تخلف و تقلب در نظام بانکی


به‌نام
خدا

فناوری‌های مالی

فصلنامه تخصصی کاربرد نوآورانه فناوری در ارائه خدمات مالی

شماره ۱

تابستان ۱۴۰۱

نشریه داخلی شرکت داتین

سردبیر: مژگان رضایی

دبیر تحریریه: فاطمه قوتی

همکاران این شماره: رضا قربانی، علی نعمتی شهاب، آرمین منتظری، محمد رحمتی، کیمیا قاسم‌زاده، سید علی طباطبایی، نیلوفر حق‌جو، علیرضا بادامچی، امین میرزایی عسگرانی، ریحانه هاشمی، نیلوفر امرایی، ستاره ارانی، روشن نوروزی

مدیر اجرایی: مریم عبادی

مدیر هنری: حامد زاهد

چاپ: چاپ دقت

آدرس: تهران، خیابان نلسون ماندلا (آفریقا)، خیابان ناهید شرقی، پلاک ۳۳ کدپستی: ۱۹۱۵۷۱۸۱۸۱

تلفن: ۲۴۵۹۷۰۰۰ (۰۲۱) نمابر: ۲۴۵۹۷۷۷۷ (۰۲۱)

ایمیل: info@dotin.ir

فهرست

چرا فصلنامه فناوری‌های مالی؟

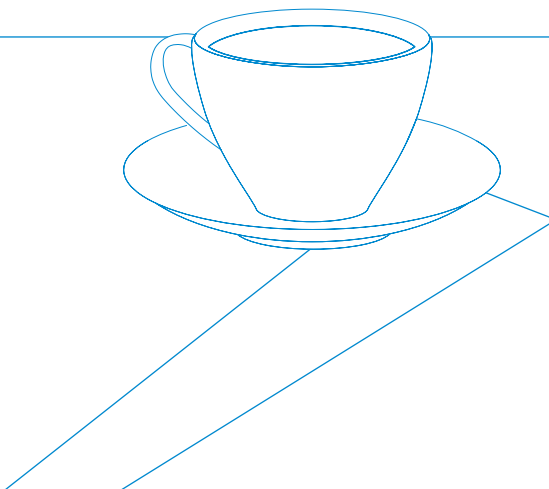
مژگان رضایی
مدیر روابط عمومی داتین

در دنیای امروز، بیش از هر زمانی رسانه‌ها به لطف دنیای مجازی در دسترس مخاطبان خود قرار گرفته‌اند و افراد هر روز و هر لحظه از «رویدادها» و «اخبار» در قالب جریان‌های خبری آگاه می‌شوند. اما در مقابل، ما امروزه نسبت به سالیان قبل، فرصت کمتری را صرف درنگ و مطالعه عمیق‌تر در مورد مفاهیم، روندها، مسیرهای تحول و آنچه فراتر از روزمرگی است و به آینده نظر دارد، می‌کنیم. در عصر تحول دیجیتال، این امر در حوزه‌های فناورانه و دانش‌بنیان به ویژه صنعت فناوری مالی که هر روز در معرض تحولات بنیادین است، چندان دوراندیشانه نیست. ما نیاز داریم تا بتوانیم به مرزهایی دورتر از امروز سر بزنیم و به راه‌های نرفته و گام‌های بعدی این صنعت تأثیرگذار، فکر کنیم.

ما در داتین به عنوان یکی از شرکت‌های متخصص فعال در بازار ارائه زیرساخت‌های فناوری مالی، همواره با چالش‌ها، پرسش‌ها و خواسته‌های مدیران و کارشناسان صنعت مالی کشور در حوزه فناوری، با نگاهی تخصصی و به دور از جنجال‌های بازار، مواجه‌ایم. اما فراتر از توسعه محصولاتمان، چگونه می‌توانیم به این پرسش‌ها پاسخی مناسب بدهیم؟

فصلنامه فناوری‌های مالی برای پاسخ به این دغدغه، گام به دنیای رسانه‌های تخصصی حوزه فناوری کشور گذاشته و قرار است فضایی باشد برای گفت‌وگو درباره موضوعات کلیدی صنعت مالی با نگاهی به امروز و آینده، روندها و تحولات جهانی صنعت فناوری مالی و مسیر طی‌شده. «فناوری‌های مالی» می‌خواهد در قالب پرونده‌های تخصصی، تریبونی باشد تا در آن، مدیران و متخصصان صنعت فناوری مالی و روزنامه‌نگاران فناوری با رویکردی علمی- کاربردی و به دور از نگاهِ خبری صرف، به طرح و تحلیل موضوعات چالش‌انگیز فناوری مالی در کشور بپردازند.

و در آخر اینکه، این فصلنامه رقیب هیچ رسانه‌ای نیست و قرار نیست تریبون تبلیغاتی شرکت یا نهادی باشد. فصلنامه فناوری‌های مالی به قول حافظ بزرگ، یک «قطره محال‌اندیش» است که رسالت خود را دعوت به بازاندیشی در صنعت فناوری مالی با نگاهی تحول‌گرا و آینده‌نگر می‌داند.



چرا سیستم‌های کشف تقلب اهمیت دارند؟

رضا قربانی
رئیس کمیسیون فین‌تک سازمان نظام صنفی رایانه‌ای استان تهران

در باب اهمیت سیستم‌های کشف تقلب به نظرم به اندازه کافی صحبت شده است؛ بعید می‌دانم مدیری در سیستم بانکی کشور وجود داشته باشد که اهمیت سامانه‌های کشف تقلب را نداند یا حاضر باشد با آن مخالفت کند. به عبارتی در ظاهر همه موافق این موضوع مهم هستند و به اندازه کافی سخنران و مروج داریم که درباره اهمیت سامانه‌های کشف تقلب صحبت می‌کنند. اما در عمل چقدر از این سامانه‌ها استفاده می‌شود؟ در عمل، چقدر مبارزه با تخلفات را از طریق سیستم‌های نرم‌افزاری انجام می‌دهیم؟ در این زمینه چقدر از هوش مصنوعی استفاده می‌کنیم؟ تکنولوژی‌های روز مانند یادگیری ماشین چقدر مورد استفاده قرار می‌گیرد؟ با یک بررسی ساده می‌توانیم پاسخ این پرسش‌ها را بیابیم. برخلاف صحبت‌هایی که می‌شنویم وضعیت استفاده از سامانه‌های کشف تقلب، قابل قبول نیست. به عبارتی به دلایل متعدد، وضعیت هوش تجاری در سیستم بانکی ایران تعریفی ندارد. این ایراد قاعدتا به بحث مقررات‌گذاری برمی‌گردد. با اینکه قوانین و مقررات بانکی در زمینه مبارزه با تقلب، دستورالعمل‌هایی دارد ولی حلقه مفقوده همه

آنها نادیده‌گرفتن تکنولوژی است. قوانین و مقررات سیستم بانکی ایران به تکنولوژی کاری ندارند و آن را صرفا ابزاری مانند بقیه ابزارها می‌بینند.
این در حالی است که تکنولوژی‌ها بسیاری از مفاهیم دنیای بانکداری را متحول کرده‌اند. تکنولوژی صرفا ابزاری نیست که برخی از آن استفاده کنند و همان کارهای قدیمی را با ابزارهای جدید انجام دهند. تکنولوژی ظرفی است که مظروف را به شکل خودش درمی‌آورد. دنیای بانکداری بعد از تکنولوژی دیگر قابل مقایسه با دنیای پیش از تکنولوژی نیست. در سیستم‌های بانکی سه ستون اصلی داریم: سیستم‌های فنی، سیستم‌های حقوقی و خوشنامی.
ما در زمینه سیستم‌های فنی کشف تقلب، پیشرفت‌های خوبی داشته‌ایم و همین امروز هم ابزارها و راه‌حل‌های خوب، به‌روز و متنوعی داریم؛ منتها چارچوب‌های حقوقی و قانونی، متناسب با ابزارهای تکنولوژیک نیستند.
با نگاهی به مسائل حقوقی مرتبط با بانک‌های کشور می‌بینیم که هنوز هم سامانه‌های نرم‌افزاری جایگاه مناسبی در مبارزه با تقلب ندارند. این در حالی است که هر شرکت و کسب‌وکار بانکی و پرداختی باید به صورت پیوسته تمام تراکنش‌ها را رصد و پردازش و با توجه به الگوریتم‌ها ریسک‌ها را شناسایی کند. بانک‌ها مهم‌ترین کارکردی که دارند خلق و نگهداری اعتماد است. آنها باید بتوانند برای همه مردم در هر شرایطی حس اعتماد ایجاد کنند. ریسک چیزی نیست که از آن فرار کنیم. ریسک چیزی است که با آن زندگی می‌کنیم. بنابراین در بررسی وضعیت موجود به نظر می‌رسد ما ترجیح می‌دهیم ریسک را نبینیم و همین فرهنگ، شرایطی را ایجاد کرده که ما برای مدیریت ریسک هزینه نمی‌کنیم. ما آنقدر در کنار ریسک‌ها زندگی کرده‌ایم که گاهی اوقات حساسیتمان را از دست داده‌ایم.
قاعدتا مثال‌های زیادی از کشورهای توسعه‌یافته داریم که نشان می‌دهد کسب‌وکارهای فعال صنعت بانکداری تا چه میزان به مدیریت ریسک اهمیت می‌دهند. موضوعاتی مانند تطبیق باعث شده که هزینه‌های بسیار زیادی برای انجام تراکنش‌ها مطابق با چارچوب‌ها انجام شود.
این مثال‌ها را در این یادداشت کوتاه باز نمی‌کنیم ولی مخاطب آگاه یا از آنها اطلاع دارد یا با یک جست‌وجوی ساده می‌تواند انبوهی از آنها را بیابد. هدف این یادداشت کوتاه این بود که بگوید سال‌هاست مسائل فنی مبارزه با تقلب حل شده است؛ آنچه که اکنون در این مرحله باید تغییر کند بحث قوانین و مقررات است. ما باید به استفاده از تکنولوژی چراغ سبز نشان دهیم. فراموش نکنیم که تکنولوژی را فقط با تکنولوژی می‌توان مهار کرد.

مقدمه‌ای بر تشخیص تقلب و تخلف در سیستم‌های بانکی و مالی

علی نعمتی شهاب
پژوهشگر تحول دیجیتال در صنعت بانکداری و پرداخت

منظور از تخلف و تقلب در خدمات مالی، بانکی و پرداخت، عبارت است از انجام هر گونه فعالیت‌های بانکی و پرداختی از روش‌های غیرقانونی از جمله استفاده از کارت‌های بانکی یا اطلاعات حساب بانکی دزدیده‌شده برای پرداخت، جعل هویت (چه در سمت پذیرنده و چه در سمت پرداخت‌کننده وجه)، فعالیت‌های نامتعارف با حساب‌های بانکی اجاره‌ای، انجام تراکنش‌های مشکوک به پولشویی و مانند آنها.

به صورت کلی مهم‌ترین انواع تقلب‌ها و تخلف‌های موجود در سیستم‌های مالی و بانکی عبارتند از:

• تقلب و تخلف در تراکنش‌های پرداخت: کلاه‌برداران ممکن است خرید آنلاین را فضای مناسبی برای امتحان‌کردن اطلاعات کارت‌های پرداخت دزدیده‌شده بیابند. درگاه‌های پرداخت محافظت‌نشده با سامانه ضد تقلب و تخلف، می‌توانند منجر به تراکنش‌های کلاه‌بردارانه قابل توجهی شوند که نتیجه آن هم ازدست‌رفتن درآمد برای مؤسسه مالی و علاوه بر آن جریمه‌های سنگین از سوی نهادهای نظارتی است. به عنوان مثال ممکن

است پذیرنده متقلب و متخلف، به جای یک صورت‌حساب، دو صورت‌حساب مشابه را به دو بخش متفاوت یک شرکت ارسال کند. واحد مالی شرکت هم متوجه نشود و این مبلغ را دو بار پرداخت کند.

• جعل هویت و استفاده از حساب دیگران: استفاده از حساب‌های دیگران ـ چه با اطلاع صاحب حساب و در قالب اجاره‌دادن حساب بانکی باشد و چه بدون اطلاع فرد و بر اساس اطلاعات دزدیده‌شده کارت یا حساب بانکی او، یکی از مهم‌ترین انواع تقلب‌ها و تخلف‌های موجود در حوزه خدمات مالی و بانکداری است. جعل هویت و استفاده از حساب افراد بدون اطلاع آنها برای عملیات کلاه‌بردارانه مالی و بانکی در سال ۲۰۲۰ بیش از ۷۲ درصد افزایش یافته است.

• فیشینگ و تظاهر به پذیرنده معتبر بودن: یکی از شایع‌ترین روش‌های تقلب و تخلف، سوء استفاده کلاه‌برداران از اعتبار برندهای شناخته‌شده یا تظاهر به پذیرنده معتبر بودن در فضای مجازی است. در این حالت، مجرم، با فریب‌دادن فرد، او را وادار به پرداخت پول به یک حساب دزدی می‌کند یا اینکه با مهندسی اجتماعی، اطلاعات حساب بانکی یا کارت بانکی فرد را به شکل مستقیم از خود او دریافت می‌کند تا از این اطلاعات برای انتقال وجه به خود یا پرداخت‌های کلاه‌بردارانه استفاده کند. بر اساس برخی آمار موجود، فیشینگ، عامل وقوع بیش از نیمی از تخلفات مالی سایبری است.

تقلب و تخلف همواره یکی از چالش‌های اصلی صنعت مالی به ویژه بانک‌ها که به پردازش تراکنش‌های مالی می‌پردازند، بوده است. دیجیتالی‌شدن زندگی و در نتیجه افزایش قابل توجه تراکنش‌های مالی مبتنی بر اینترنت، باعث شده تا راه‌های جدیدی برای تقلب و تخلف پدید آید که نتیجه آن هم افزایش جرایم مالی بوده است. اگر قبل از این برای تقلب مالی به دسترسی به جسم فیزیکی کارت ملّی یا کارت بانکی افراد نیاز بود، امروزه تنها با دسترسی به نام کاربری و رمز حساب بانکی افراد، می‌توان پول‌های آنها را سرقت کرد.

همین‌جا لازم است اشاره کنیم که تقلب و تخلف تنها مربوط به حوزه بانکی و پرداخت نیست و در واقع تمامی مؤسسات مالی (مانند بیمه‌ها و کارگزاران بورس) و حتی غیر مالی (تمامی شرکت‌های دارای فرایندهای دریافت و پرداخت وجه به ویژه پذیرندگان آنلاین مانند فروشگاه‌ها و بازارگاه‌های اینترنتی) در معرض خطر وقوع تقلب و تخلف مالی هستند.

تشخیص تقلب و تخلف و اهمیت آن در دنیای امروز

تشخیص تقلب و تخلف عبارت است از فرایند تشخیص تراکنش‌هایی که به دنبال جابه‌جایی پول یا منابع اعتباری به صورت غیرقانونی و غیرمجاز، ولی با وانمودکردن

درست و قانونی بودن مبدأ، مقصد و ماهیت تراکنش هستند. تشخیص تقلب و تخلف با کمک تکنیک‌ها و ابزارهای یادگیری ماشین و تحلیل داده اجرا می‌شود و به دنبال کشف تراکنش‌های مشکوک است.

منظور از تراکنش مشکوک عبارت است از ورود پول به حساب اشخاص (اعم از حقیقی و حقوقی)، به شکلی که مبدأ و منشأ و علت واریز آن وجه به حساب فرد، برای بانک مشخص نباشد. به بیان دیگر، اگر فرد بابت وجه واریزی به حساب خود، نتواند اسناد و مدارک معتبری برای اثبات قانونی و مجازبودن آن ارائه بدهد، این پول یک تراکنش مشکوک لحاظ می شود.

بررسی‌ها نشان می‌دهد که اغلب گونه‌های تقلب و تخلف مالی در قالب دزدی یا جعل هویت رخ می‌دهند. بر اساس پژوهش‌های انجام‌شده، در سال ۲۰۲۰ حدود ۲.۲ میلیون گزارش وقوع تقلب و تخلف از سوی مشتریان (با ادعای خسارتی بالغ بر ۳.۳ میلیارد دلار) توسط مؤسسات مالی آمریکایی دریافت شده است. در همین سال که اوج دوران بحران کرونا بود، چیزی حدود ۴۰۰ میلیارد دلار حقوق بیکاری افراد و ۱۰۰ میلیارد دلار از حمایت‌های مالی دولتی مربوط به کرونا هم به سرقت رفته است. همچنین بر اساس برخی برآوردها مجموع خسارت مؤسسات مالی بابت تقلب و تخلف جعل هویت هم در همین سال به عددی بالغ بر ۵۶ میلیارد دلار رسیده است.

خبر بد این است که هیچ نشانه‌ای از کُندشدن این روند هم مشاهده نمی‌شود و روندهای جهانی هم به سوی افزایش احتمال وقوع تقلب و تخلف مالی هستند:

• حجم تراکنش‌های آنلاین (به ویژه تراکنش‌های انجام‌شده روی گوشی‌های هوشمند افراد) در حال افزایش با نرخ سالیانه حدود ۴۲ درصد است و در نتیجه فرصت‌های بیشتری برای تقلب و تخلف در اختیار کلاه‌برداران قرار گرفته است.

• پیشرفت فناوری باعث پیشرفته‌ترشدن روش‌های تقلب و تخلف و افزایش جرایم مالی سایبری شده است. به عنوان مثال گفته می‌شود که در ایالات متحده هر ۳۹ ثانیه یک حمله هکری اتفاق می‌افتد، تعداد حملات به حساب‌های بانکی افراد با نرخ سالانه ۷۲ درصد در حال افزایش است و اطلاعات حداقل نیمی از شهروندان آمریکایی هم در نشت داده‌های اتفاق افتاده در طول پنج سال اخیر در اینترنت افشا شده است.

• تقلب و تخلف فقط خاص حوزه مالی و بانکی نیست و حوزه‌های دیگر هم تحت تأثیر آن قرار گرفته‌اند. از جمله خرده‌فروشی (با نرخ رشد سالانه ۶۱ درصد)، تجارت الکترونیکی (با نرخ رشد سالانه ۸۳ درصد)، وام‌گیری آنلاین (با نرخ رشد سالانه ۴۰ درصد) و عملیات مالی آنلاین (با نرخ رشد سالانه ۵۸ درصد).

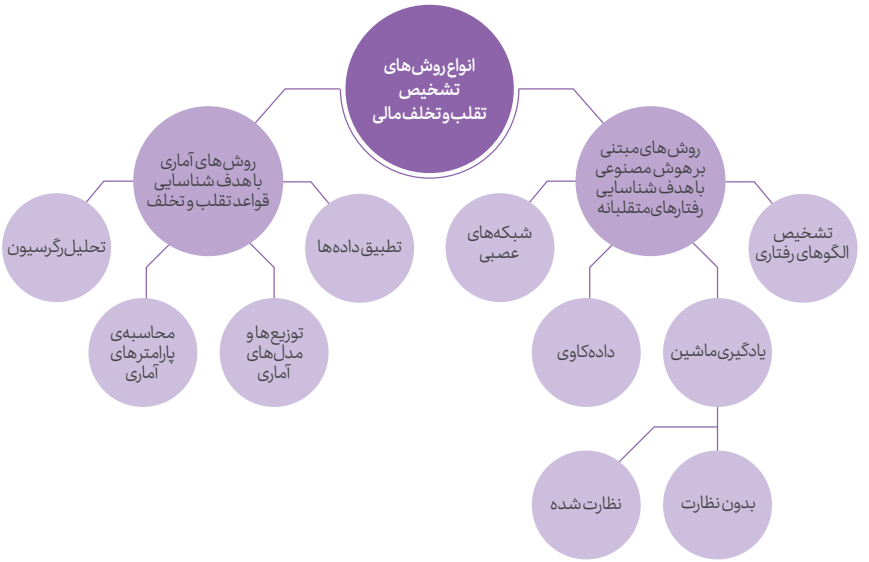
نکته بسیار مهم دیگر این است که بر اساس برخی پژوهش‌ها حداقل ۲۰ درصد مشتریان،

1. Fraud Detection

پس از آسیب‌دیدن از هر گونه جرم مالی، بانک خود را تغییر می‌دهند. بنابراین شناسایی تقلب و تخلف به صورت بلادرنگ و در زمان وقوع تراکنش‌ها، فراتر از جلوگیری از ایجاد چالش با نهادهای نظارتی از جمله بانک مرکزی و پیشگیری از جریمه‌های سنگین مالی ناشی از آن، بلکه برای حفظ جایگاه برند مؤسسه مالی و پایگاه مشتریان آن، امری کاملا ضروری به حساب می‌آید.

بررسی روش‌های تشخیص تقلب و تخلف مالی: محافظت مبتنی بر قواعد[۲] در برابر یادگیری ماشین

تمام سامانه‌های تشخیص تقلب و تخلف به صورت مشابه با هم کار نمی‌کنند؛ با این حال به صورت کلی می‌توان روش‌های تشخیص تقلب و تخلف مالی را به دو دسته کلی تقسیم کرد:



در ادامه به بررسی دو روش کلی تشخیص تقلب و تخلف مالی می‌پردازیم:

الف. روش‌های آماری با هدف شناسایی قواعد تقلب و تخلف

قبل از به‌کارگیری یادگیری ماشین در این حوزه، سازوکارهای مبتنی بر قواعد تشخیصی

2.The rule-based Protection

مورد استفاده قرار می‌گرفتند و هنوز هم این رویکرد در سامانه‌های تشخیصی بانک‌ها و مؤسسات مالی در حال استفاده است. در این سامانه‌ها قواعد مربوط به تراکنش‌ها و فعالیت‌های مشکوک در یک پایگاه داده نگهداری می‌شود و اگر سامانه بانکی یا مالی، به یک تراکنش یا فعالیت بربخورد که با قواعد تعریف‌شده مشابهت دارد، آن تراکنش یا فعالیت را مسدود می‌کند. به صورت معمول، قواعد شناسایی تخلف بر اساس تحلیل‌های آماری برای شناسایی سناریوهای ریسک بروز تقلب و تخلف توسط کارشناسان متخصص این حوزه نوشته می‌شود.

بر اساس برخی ارزیابی‌ها به صورت متوسط حدود ۳۰۰ قاعده تشخیص تقلب و تخلف در سامانه‌های مالی امروز برای تائید یک تراکنش مورد بررسی قرار می‌گیرد. به همین دلیل، عموما سامانه‌های مالی نمی‌توانند آنها را در لحظه مورد بررسی قرار دهند. بنابراین معمولا تراکنش‌های مشکوک را تائید می‌کنند تا در صورت بروز مشکل و درخواست دستگاه‌های نظارتی، بعدا به آن رسیدگی کنند.

مشکل اصلی این نوع تشخیص تقلب و تخلف این است که کلاه‌برداران خیلی سریع قواعد مربوط به این رویکرد را شناسایی می‌کنند و با تغییر روش‌های تقلب و تخلف خود، از شناسایی‌شدن توسط سامانه تشخیص تقلب و تخلف می‌گریزند. بنابراین دوباره به شناسایی سناریوهای ریسک جدید، طراحی قواعد و پیاده‌سازی آن در سامانه‌های مالی نیاز است که امری زمان‌بر و هزینه‌بر است.

ب. روش‌های مبتنی بر هوش مصنوعی با هدف شناسایی رفتارهای متقلبانه

روش مبتنی بر هوش مصنوعی بر اساس شناسایی «الگوهای رفتاری»[3] کار می‌کند و تهدیدها را پیش از اینکه بتوانند هر گونه آسیبی ایجاد کنند، متوقف می‌کند. هوش مصنوعی به جای اینکه فقط به ساختار تراکنش توجه کند، بستر[4] انجام تراکنش و روابط پس‌زمینه‌ای آن را بررسی می‌کند تا بتواند به احتمال وجود رفتار تقلب و تخلف‌آمیز پی ببرد. این تحلیل‌ها می‌تواند بر اساس متغیرهایی چون نوع تراکنش پرداخت، اینکه پذیرنده پرداخت آیا قبلا از پرداخت‌کننده پولی دریافت کرده یا نه، تطبیق میزان مبلغ تراکنش با نوع تراکنش اظهارشده، محل انجام تراکنش، زمان انجام تراکنش و مانند آنها باشد.

ویژگی مهم روش مبتنی بر هوش مصنوعی این است که می‌تواند حجم عظیمی از تراکنش‌ها را در لحظه مورد تحلیل قرار دهد و در نتیجه از وقوع جرم، جلوگیری کند. به همین دلیل، مراحل و زمانِ تائید تراکنش‌ها را به‌شدت کاهش می‌دهد. مزیت دیگر این رویکرد این است که سامانه به صورت دائمی در حال به‌روزرسانی سناریوهای تقلب و تخلف و قواعد شناسایی آنها به صورت خودیادگیری است.

3.Behavioral Patterns 4.Context

جدول زیر تفاوت‌های میان دو رویکرد کلی تشخیص تقلب و تخلف را نشان می‌دهد:

روش مبتنی بر قواعد	روش مبتنی بر هوش مصنوعی
دنبال‌کردن سناریوهای واضح تقلب و تخلف	شناسایی روابط و هم‌بستگی‌های پنهان‌شده در حجم عظیم داده‌ها
نیازمند به‌روزرسانی دستی قواعد برای مقابله با سناریوها و ریسک‌های جدید تقلب و تخلف	شناسایی خودکار سناریوهای ریسک جدید و احتمالی بروز تقلب و تخلف
نیازمند چند مرحله گوناگون برای تائید تراکنش‌ها که تجربه مشتری را تضعیف می‌کند	کاهش قابل توجه مراحل تائید تراکنش
نیازمند پردازش طولانی مدت تراکنش‌ها برای کشف تقلب و تخلف	پردازش لحظه‌ای تراکنش‌ها برای کشف تقلب و تخلف

با توجه به اینکه عموما سامانه‌های تشخیص تقلب و تخلف در دنیای امروز بر اساس یادگیری ماشینی عمل می‌کنند، در ادامه به بررسی این رویکرد به عنوان نمونه چگونگی کارکرد یک سامانه تشخیص تقلب و تخلف می‌پردازیم:

چگونگی کارکرد تشخیص تقلب و تخلف توسط یادگیری ماشینی

سامانه تشخیص تقلب و تخلف مجموعه‌ای از ابزارهای مبتنی بر یادگیری ماشین، تحلیل آماری و پایش رفتاری را به کار می‌گیرد تا بتواند الگوها و راهبردهای تقلب و تخلف مورد استفاده توسط کلاه‌برداران را تشخیص دهد. زمانی که پیش‌نیازهای وقوع تقلب و تخلف شناسایی شوند، سامانه می‌تواند هر گونه تقلب و تخلفی را پیش از ورود آسیب، شناسایی کند.

برای این منظور، مجموعه‌های عظیمی از داده توسط الگوریتم هوش مصنوعی و بر اساس متغیرهای مختلف مؤثر بر تقلب و تخلف مورد بررسی قرار می‌گیرد تا همبستگی نهفته موجود بین رفتار کاربران و احتمال وقوع جرایم مالی شناسایی شوند. در این راستا سامانه کشف تقلب و تخلف، در ابتدا بر اساس تحلیل آماری داده‌های رفتار تقلب و تخلف‌آمیز گذشته، الگوهای رفتاری تقلب و تخلف‌آمیز را شناسایی می‌کند و برای هر نوع رفتار، یک ضریب ریسک مشخص را محاسبه می‌کند. این ضریب ریسک شامل تعیین اینکه یک نوع تراکنش خاص، چقدر احتمال دارد تقلب و تخلف‌آمیز باشد، بر اساس متغیرهای پیش‌بینی‌کننده موجود در تراکنش‌های مالی است.

برای کارکرد اثربخش تشخیص تقلب و تخلف، سامانه ابتدا باید نمونه‌هایی از تقلب‌ها و تخلف‌های شناخته‌شده را بررسی کند. در اینجا به برخی از مدل‌های معمول یادگیری

ماشین در تشخیص تقلب و تخلف اشاره می‌کنیم:

۱- طبقه‌بندی نظارت‌شده

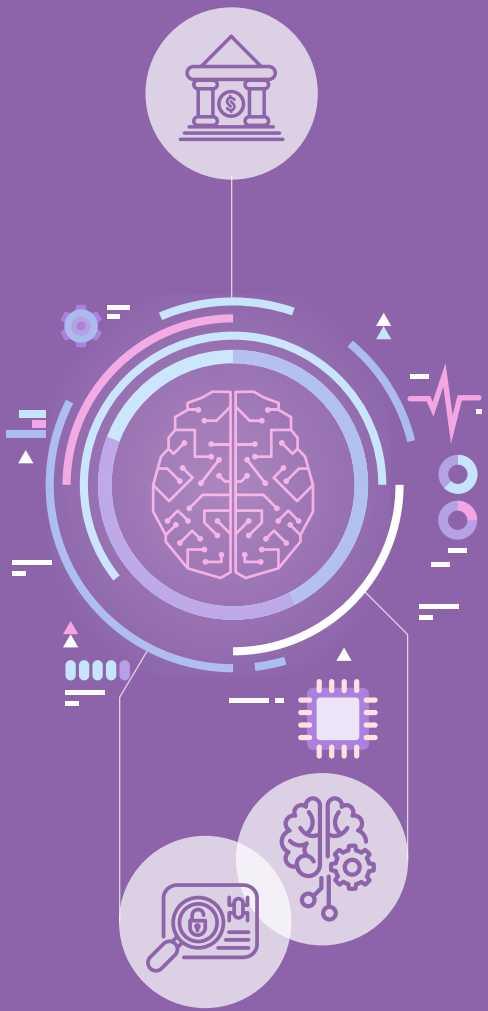
یادگیری نظارت‌شده عبارت است از آموزش‌دادن یک الگوریتم برای تشخیص تقلب و تخلف بر اساس داده‌های تاریخی. فرایند آموزش از مجموعه داده‌هایی که در آنها متغیرهای مرتبط با تقلب و تخلف، نشانه‌گذاری شده‌اند انجام می‌شود تا بدین ترتیب پژوهشگران بتوانند میزان موفقیت یک الگوریتم جدید را در تشخیص تقلب و تخلف، اندازه‌گیری کنند.

این روش آموزش الگوریتم به پژوهشگران اجازه می‌دهد تا متغیرهایی که الگوریتم بر اساس آنها یاد می‌گیرد را کنترل کنند و به این ترتیب، یک چارچوب ساده را برای آزمون و خطا و اصلاح الگوریتم در طی فرایند یادگیری ماشین، ایجاد کنند.

۲- طبقه‌بندی بدون نظارت

طبقه‌بندی بدون نظارت داده‌های بدون برچسب را در طبقه‌های مختلف بر اساس روابط میان سرفصل‌های داده‌ای موجود در یک مجموعه داده مرتب می‌کند. روابط پنهان میان داده‌ها در این فرایند تحلیلی شناسایی می‌شوند و بدین ترتیب می‌توان الگوهای جدید فعالیت‌های تقلب و تخلف‌آمیز را شناسایی کرد.

این روش تشخیص تقلب، نیاز به برچسب‌گذاری داده‌ها را از بین می‌برد؛ فعالیتی که بسیار زمان‌بر است. در عین حال این رویکرد می‌تواند باعث شود تا



5.Ccorrelation

الگوریتم، تعدادی الگوهای غیرضروری را هم یاد بگیرد که به فرایند تشخیص تقلب و تخلف کمکی نمی‌کنند.

جمع‌بندی: ویژگی‌های سامانه‌های اثربخش تشخیص تقلب و تخلف

تشخیص تقلب و تخلف یکی از مهم‌ترین پیش‌نیازهای موفقیت بانک‌ها و مؤسسات مالی در دنیای امروز است؛ چه از زاویه دید رعایت قوانین و مقررات (تطبیق)[6] و چه از زاویه دید تجربه مشتری. امروزه مؤسسات مالی برای شناسایی تقلب و تخلف از سامانه‌های تخصصی طراحی‌شده برای تشخیص تقلب و تخلف به صورت بلادرنگ استفاده می‌کنند. یک سامانه اثربخش در این حوزه باید ویژگی‌های زیر را داشته باشد:

- دارای پایگاه داده قدرتمند و به‌روز شامل الگوریتم‌ها، الگوها و قواعد تحلیل ریسک تقلب و تخلف به همراه قابلیت به‌روزرسانی پایگاه داده توسط متخصصین یا به صورت سیستمی (بر اساس یادگیری ماشین)
- توانایی تشخیص و کشف تقلب و تخلف در لحظه
- دارای داشبورد نمایش وضعیت و آمار تقلب و تخلف‌های شناسایی‌شده در لحظه همراه با قابلیت گزارش‌گیری
- منطبق بر آخرین قوانین و مقررات و استانداردهای داخلی و بین‌المللی بانکی و مالی در حوزه‌های مختلف؛ اعم از: تشخیص تقلب و تخلف، مدیریت ریسک‌های اعتباری و مبارزه با پولشویی و تأمین مالی تروریسم
- قابلیت تحلیل داده‌ها به منظور شناسایی روابط و هم‌بستگی‌های پنهان در داده‌ها با هدف یادگیری مستمر و به‌روزرسانی سناریوهای ریسک تقلب و تخلف به صورت خودکار بر اساس یادگیری ماشین

منابع:

https://www.outseer.com/fraud-protection/fraud-protection-fraud-detection/
https://www.altexsoft.com/whitepapers/fraud-detection-how-machine-learning-systems-help-reveal-scams-in-fintech-healthcare-and-ecommerce/
https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-fraud-detection/
https://www.inscribe.ai/fraud-detection

6.Compliance

تقلب و تخلف در صنعت بانکداری: سهل یا ممتنع؟

ریحانه هاشمی
خبرنگار

صنعت بانکداری، یکی از صنایعی است که در طول دو دهه گذشته و به لطف گسترش استفاده از اینترنت، رشد کمی و توسعه کیفی زیادی را تجربه کرده است. گسترش خدمات بانکی و سادگی روزافزون استفاده از آنها، در کنار فرصت‌های بسیاری که برای بانک‌ها و مشتریانشان به وجود آورده، باعث صرفه‌جویی‌هایی در وقت و هزینه افراد شده اما تهدیدهایی را هم در بر داشته است. تهدیدهایی که زمینه را برای کلاه‌برداری‌های کوچک و بزرگ فراهم کرده است. در این گزارش به بحث «تقلب و تخلف در صنعت بانکداری» می‌پردازیم.

تقلب و تخلف، اغلب در کنار هم به کار برده شده و هم‌معنی دانسته می‌شوند. اما در سیستم بانکی، این دو کلمه معانی جداگانه‌ای دارند و زمینه استفاده از آنها هم متفاوت است. تخلف، آنچنان که از اسمش برمی‌آید، به معنای انجام کاری است که خلاف قانون بوده و با متن قانون در تضاد است. مثال‌های زیادی از تخلف در صنعت بانکی وجود دارد

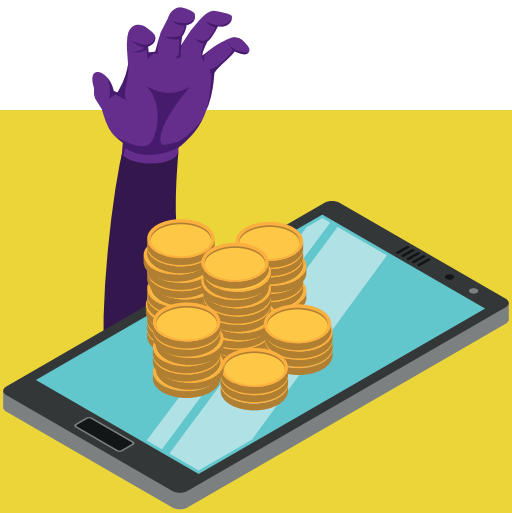
که از جمله آنها می‌توان به هک‌کردن رمز اینترنت‌بانک مشتریان یک بانک اشاره کرد.
تقلب اما زمانی اتفاق می‌افتد که فرد در ظاهر، مرتکب کاری نشده که بتوان به آن عنوان «خلاف قانون» را اطلاق کرد، اما کارش به نوعی دور زدن قانون است. مثل استفاده یک فرد از حساب‌های دیگران برای جلوگیری از اینکه بتوان گردش‌های مالی او را رصد کرد. تقلب هرچند به خودی خود خلاف قانون نیست، اما منجر به منفعت مالی برای فرد یا یک عده و ضرر و زیان برای فرد یا گروهی دیگر می‌شود.
نمی‌توان مبدا درستی از بازشدن پای تقلب و تخلف در صنعت بانکداری کشور ارائه داد اما اختلاس ۱۲۳ میلیاردی بانک صادرات که در بین سال‌های ۱۳۷۱ تا ۱۳۷۳ اتفاق افتاد، شاید اولین تخلف مهم در بانکداری کشور باشد. این رویداد مربوط به زمانی بود که سیستم بانکداری کشور هنوز به صورت یکپارچه درنیامده بود و بانکداری الکترونیک، هنوز به معنای امروزی مورد استفاده قرار نگرفته بود.
آن زمان هنوز اینترنت وجود نداشت و هیچ یک از خدمات بانکی بر بستر اینترنت ارائه نمی‌شد. حالا با فراگیری عجیب استفاده از اینترنت برای فعالیت‌های بانکی، اوضاع بسیار متفاوت با گذشته است و بحث تقلب و تخلف در بانکداری نیز معنایی گسترده‌تر از اختلاس‌های میلیاردی دارد.
در گذشته، باور اینکه خدمات بانکی قرار است در آینده نزدیک این‌چنین متحول و دگرگون شود و استفاده از آنها بسیار راحت‌تر از گذشته شده و نیاز به مراجعه حضوری به بانک‌ها کمتر شود، بسیار دور از تصور بود. اما امروز، بسیاری از خدمات بانکی، بر بستر اینترنت‌بانک‌ها، بدون نیاز به مراجعه حضوری به شعبات و در هر ساعتی از شبانه‌روز قابل انجام است.
دسترسی تمام افراد جامعه به کارت‌های بانکی و اینترنت‌بانک، همان‌قدر که باعث ساده‌ترشدن خدماتی مثل واریز و برداشت، پرداخت قبض و جریمه، پرداخت اقساط تسهیلات و... شده، باعث شده که افراد سودجو و کلاه‌بردار، راحت‌تر بتوانند دست به اقدامات غیرقانونی بزنند و در عین حال، کمتر ردپایی هم از خودشان به جا بگذارند.
آنچه که در گذشته به عنوان تخلف بانکی شناخته می‌شد، معمولا شامل جابه‌جایی ارقام بزرگی بود که در سطوح بالای بانکی و توسط افراد شناخته‌شده و صاحب نفوذ انجام می‌گرفت. اما تخلف و تقلب در دوران حاضر، تخلف‌هایی با ارقام بزرگ نیست. گستردگی استفاده از خدمات مالی بر بستر اینترنت، بسیاری از افراد را به این فکر انداخته که با روش‌های ساده و با استفاده از ناآگاهی مردم، مرتکب تخلف‌های کوچک ولی متعدد بانکی شوند.

تقلب در بانکداری الکترونیکی

تقلب در بانکداری الکترونیکی، در بستر خدمات الکترونیکی و به صورت آنلاین اتفاق می‌افتد. تعریف این نوع تقلب، انتقال پول الکترونیکی به صورت آنلاین از یک حساب به حساب دیگر، به صورت نامشروع، غیرقانونی، بدون اطلاع و رضایت صاحب حساب مبدا است. به طور کلی، اینترنت‌بانک‌ها، پایانه‌های فروش، دستگاه‌های خودپرداز و اپلیکیشن‌های موبایلی بانک‌ها، درگاه‌هایی هستند که تقلب و تخلف از طریق آنها انجام می‌شود.

سیستم‌های مالی مبتنی بر فناوری اطلاعات به دلیل پتانسیل بالایی که برای سرقت پول در حجم زیاد دارند، اهداف راحتی برای تقلب هستند. افراد متقلب و سودجو نیز از نقص‌های متعدد در سامانه‌های احراز هویت یا نقاط ضعف موجود در مدل‌های امنیتی در سرویس‌ها استفاده کرده و بدون اینکه خطر چندانی برای ردیابی آنها را تهدید کند، دست به تقلب و جابه‌جایی پول می‌زنند. از سوی دیگر، احراز هویت ضعیفی که توسط سازوکارهای امضا، رمز عبور و کد امنیتی کارت اتفاق می‌افتد، تراکنش‌های غیرقانونی را ساده‌تر می‌کند.

کلاه‌برداری یا تقلب در بانکداری الکترونیکی، معضلی است که گریبان بانک‌های مختلف در سراسر دنیا را گرفته است. در بعضی موارد، تقلب در بانکداری الکترونیکی باعث ورشکستگی برخی بانک‌ها شده و سهم مهمی از دارایی‌های بانک‌ها را از دست آنها خارج کرده است. گزارش‌ها نشان می‌دهد بیش از نیمی از بانک‌های جهانی که در صنعت بانکداری خرد مشغول به کار هستند، در سال‌های ۲۰۱۸ و ۲۰۱۹ با افزایش تقلب و کلاه‌برداری روبه‌رو شده‌اند. با افزایش تراکنش‌های مربوط به یک بانک، احتمال تقلب و کلاه‌برداری به صورت معنادار افزایش پیدا می‌کند.



روش‌های معمول در تقلب بانکی

روش‌های مختلف و متعددی برای تقلب در بانکداری شناخته شده و توسط کلاه‌برداران مورد استفاده قرار گرفته است. اما بعضی از این روش‌ها دربرگیری بیشتری داشته‌اند و تعداد دفعاتی که از آنها استفاده شده، بیشتر است. یکی از این روش‌ها، استفاده از اطلاعات هویتی افراد برای دسترسی به حساب‌های بانکی آنهاست. این روش در دنیا مهم‌ترین روش کلاه‌برداری و تخلف در بانکداری است. در صورتی که هکرها بتوانند به اطلاعات شخصی افراد مانند شماره شناسنامه، کد ملی، ایمیل، رمز عبور، شماره تلفن همراه و... دسترسی پیدا کنند، می‌توانند اطلاعات این افراد را جعل کرده و با استفاده از آنها، عملیات بانکی انجام دهند، بدون اینکه صاحب این اطلاعات متوجه شود.

روش بعدی، درخواست انتقال پول است. معمولا طی یک تماس به فرد گفته می‌شود که او برنده مبلغی پول نقد شده، لازم است به عابربانک مراجعه کند و دستوری را که فرد تماس‌گیرنده می‌دهد اجرا کند تا مبلغ جایزه به حسابش واریز شود. یا اینکه به فرد گفته می‌شود شماره کارت، کد CVV و تاریخ انقضای کارتش را اعلام کند و سپس کدی که به موبایلش فرستاده شده (همان رمز دوم پویا) را برای تماس‌گیرنده بخواند. در صورت اعلام رمز دوم، تمام اطلاعات لازم برای انتقال وجه اینترنتی برای تماس‌گیرنده فراهم شده و او می‌تواند حساب مورد نظرش را خالی کند.

روش معمول دیگر تخلف مالی در کشور ما، توسط فروشنده‌های آنلاین صورت می‌گیرد. این افراد کالایی را در اینترنت برای فروش می‌گذارند و از خریدار می‌خواهند مبلغ خرید را به حساب آنها واریز کند تا کالا برایش ارسال شود. مبلغ واریز می‌شود اما هیچ کالایی برای خریدار فرستاده نمی‌شود و فرد متقلب، تمام راه‌های تماس با خودش را بعد از دریافت وجه، مسدود می‌کند.

فیشینگ هم روش معمول دیگری است که کلاه‌بردار با استفاده از اطلاعات شخصی افراد، از آنها در جهت جابه‌جایی غیرقانونی پول استفاده می‌کند. در کشور ما با برقراری قانون استفاده از رمز دوم پویا برای خرید و انتقال وجه اینترنتی، معضل فیشینگ تا حد زیادی حل شده است.

نقش بانک مرکزی در مقابله با تخلف و تقلب

با توجه به گستردگی روزافزون تخلفات مالی و بانکی و افزایش تعداد مال‌باختگان، این سوال پیش می‌آید که مقصر اصلی این تخلفات کیست؟ آیا بانک مرکزی باید با تصویب آیین‌نامه‌ها و وضع مقررات، جلوی این تخلفات را بگیرد یا لازم است بانک‌ها با بالابردن سطوح امنیتی خود، جلوی لورفتن اطلاعات مشتریان را بگیرند، یا اینکه مردم می‌بایست اطلاعات خود را درباره روش‌های تخلف بالا ببرند و در دام کلاه‌برداران نیفتند؟

بانک مرکزی می‌گوید با وضع عوارض یا مالیات بر تراکنش‌های بانکی مخالف است، اما در عین حال هشدار می‌دهد مردم اطلاعات حساب بانکی‌شان را در اختیار دیگران قرار ندهند. مهران محرمیان، معاون فناوری‌های نوین بانک مرکزی، می‌گوید: «سیاست بانک مرکزی این است که هر گونه تغییر در حوزه فناوری‌های نوین بانکی با هدف ارتقای امنیت و شفافیت و بدون کمترین زحمت و دردسر برای مردم صورت پذیرد.»

به گفته محرمیان، وظایف بانک مرکزی در مبارزه با تقلب و تخلف به قوت خودش باقی است اما مردم هم باید مراقب تخلف سودجویان باشند. او می‌گوید: «وقتی کسی بابت اجاره یک حساب بانکی، چند میلیون تومان به حساب فرد صاحب حساب واریز می‌کند، صدها برابر آن پولی که پرداخته سود می‌کند اما مسئولیت ناشی از سود صدها برابری او را فردی باید بپذیرد که حسابش را اجاره داده است.»

بانک مرکزی در سال‌های اخیر، اقداماتی برای مبارزه با تخلفات بانکی انجام داده که مهم‌ترین آنها، الزام مشتریان به استفاده از رمز دوم پویا بوده است. به گفته مقامات بانک مرکزی، رمز پویا یک تکه کوچک از یک پازل بزرگ به حساب می‌آید. رمز پویا نه گام اول بوده و نه گام آخر، بلکه بخشی از یک فرایند و ناشی از یک جراحی بزرگ است.

معاون فناوری‌های نوین بانک مرکزی توضیح می‌دهد: «بعد از آن ما به سراغ ارتقای امنیت تراکنش‌ها رفتیم، به نحوی که خدمات مورد ارائه تحت تأثیر این تغییر مهم قرار نگیرد. مثلا هنگام ارسال پیامک رمز پویا، اطلاعات دارنده حساب مقصد و جزئیات آن هم برای دارنده حساب پیامک می‌شود، بدون اینکه مردم به‌زحمت بیفتند.»

اما نباید فراموش کنیم که رمز پویا، فقط می‌تواند جلوی یکی از انوع تخلف‌های بانکی را بگیرد. آیا بانک مرکزی برای جلوگیری از سایر تخلفات هم چاره‌ای اندیشیده است؟ مهران محرمیان پیش‌تر گفته بود که بانک مرکزی، بحث اعتبارسنجی مشتریان را هم دنبال می‌کند و پیشرفت‌های خوبی هم در این زمینه اتفاق افتاده است.

علاوه بر این، بانک مرکزی نوید اتفاقات مهم‌تری را هم در حوزه کشف تقلب در شبکه بانکی داده است. این بانک، در حال راه‌اندازی سامانه‌های هوشمند کشف جرائم بانکی است و مرکزی به نام مرکز واکنش سریع و عملیات مشکوک موسوم به «وسعت» ایجاد کرده که در آن، کارشناسان پلیس فتا و معاونت فضای مجازی دادستانی کل کشور، همراه بانک مرکزی هستند. محرمیان درباره این مرکز می‌گوید: «اگر چند سال پیش حساب بانکی فردی را خالی می‌کردند، رسیدگی به این پرونده چندین هفته طول می‌کشید و فرد متخلف ممکن بود تا آن زمان، رد خود را پاک کند؛ اما با تاسیس مرکز وسعت، فاصله بین وقوع جرم تا شناسایی و صدور حکم قضایی به حداقل ممکن خواهد رسید. مرکز وسعت پرونده‌ها یا تراکنش‌های مشکوک را به‌سرعت شناسایی و به آنها رسیدگی می‌کند و جلوی نقل‌وانتقال پول کثیف را می‌گیرد.»

لزوم آگاه‌سازی مشتریان بانک‌ها

پشتوانه بسیاری از تخلفات و تقلب‌ها که در بستر بانکداری الکترونیک اتفاق می‌افتد، جهل و ناآگاهی مردم است که مشتریان بانک‌ها محسوب می‌شوند. جبران خسارت تقلب برای مشتریان بانک‌ها و برگرداندن پولی که از دست داده‌اند، نه فقط در کشور ما، که در تمام جهان، احتمال کمی دارد و در بهترین حالت، کمتر از ۲۵ درصد از آنها جبران می‌شود. بنابراین همچنان نقش پیشگیری مهم‌تر از جبران است.

لازمه پیشگیری از برخی جرائم بانکی هم آگاهی‌دادن به مشتریان و مطلع‌کردن آنها از انواع تخلفات بانکی و دادن آموزش‌های لازم برای مقابله با آنهاست. مثلا چک‌کردن دقیق اطلاعات حساب شامل مبالغ واریز و برداشت‌شده، بررسی دقیق پیامک‌های واریز و برداشت و پیامک‌های مربوط به رمز دوم پویا، نادیده‌گرفتن تماس‌هایی که خبر از برنده‌شدن فرد در قرعه‌کشی می‌دهد و عدم تماس با این شماره‌ها، از جمله کارهایی است که می‌تواند به پیشگیری از تخلف و تقلب کمک کند.

علاوه بر مشتریان، بانک‌ها نیز موظفند تا با بالابردن سطح امنیت وب‌سایت‌ها و اپلیکیشن‌های موبایلی، جلوی وقوع تخلف و تقلب را بگیرند. استفاده از سامانه‌های کشف تقلب و تخلف نیز به کاهش جرایم بانکی کمک خواهد کرد. البته نباید فراموش کنیم که کشف تخلف و تقلب در بانک‌ها، در انتهای هر روز و پس از انجام تراکنش‌ها بررسی می‌شود، اما پیشگیری از تخلف و تقلب به این معناست که نباید تراکنش مشکوک اتفاق بیفتد. یعنی تراکنش مشکوک، پیش از انجام، شناسایی شده و جلوی انجام‌شدن آن تراکنش گرفته می‌شود.

پیشگیری از تخلف و تقلب نیازمند وجود برخی الزامات و قوانین بالادستی در این حوزه است. سامانه‌های کشف تخلف و تقلب می‌توانند قوانین مشخص‌شده را شناسایی و با توجه به صلاح‌دید بانک‌ها، ریسک‌ها را کاهش دهند.

از سوی دیگر، این سامانه‌ها ممکن است در تشخیص تخلف و تقلب، اشتباه کنند و باعث انجام مواردی شوند که تبعات قانونی برای بانک‌ها داشته باشد. بنابراین نباید این تصور به اشتباه ایجاد شود که سامانه کشف تخلف و تقلب نیز بدون چالش است. اما نکته مهم این است که استفاده از این سامانه‌ها، ریسک تقلب و تخلف را برای بانک به‌شدت کاهش می‌دهد.

انواع تخلف و تقلب در حوزه بانکداری

واحد مطالعات و تحقیقات داتین

انواع مختلفی از تخلف و تقلب، صنعت بانکداری را در جهان امروز مورد تهدید خود قرار می‌دهند. در ادامه انواع تخلف و تقلب را در بخش‌های مختلف خدمات بانکی بررسی می‌کنیم.

انواع تخلف و تقلب در حوزه بانکداری آنلاین

الف. دزدی اطلاعات شخصی (فیشینگ = Phishing)

فیشینگ عبارت است از تلاش مجرمان برای «ماهی‌گیری» از طریق سوءاستفاده از اطلاعات بانکی مشتریان بانک. برای این منظور، مجرمان عموما با ارسال یک ایمیل یا پیامک جعلی به افراد که به نظر می‌رسد متعلق به یک منبع مطمئن مانند خود بانک است ـ تلاش می‌کنند تا به اطلاعات بانکی آنها دست یابند. این ایمیل یا پیامک جعلی به گونه‌ای است که فرد دریافت‌کننده مشتاق می‌شود تا روی لینکی که در متن آن آمده کلیک کند. کلیک‌کردن باعث می‌شود تا فرد به یک سایت تقلبی هدایت شود که در آن از

او خواسته می‌شود تا اطلاعات بانکی خود را وارد کند. این سایت تقلبی از نظر ظاهری کاملا مشابه صفحه ورود (Log On) بانک یا صفحه درگاه پرداخت الکترونیکی طراحی شده تا به عنوان یک سایت معتبر به‌نظر برسد.
بدین ترتیب، فرد، با گمان اینکه این سایت، یک سایت معتبر است، اطلاعات بانکی یا کارت پرداخت خود را در آن وارد می‌کند؛ اما در واقع با برداشت مبالغ غیرمجاز از حساب بانکی یا کارت پرداخت وی توسط مجرم پشت پرده آن سایت تقلبی، قربانی حمله فیشینگ می‌شود.
امروزه با گسترش دسترسی به سامانه‌های ارسال پیامک و ایمیل انبوه از طریق اینترنت، مجرمان می‌توانند به سرشماره‌های مشابه شماره پیامک بانک‌ها یا نشانی‌های ایمیل ظاهرا معتبر (که در واقع نشانی‌هایی جعلی هستند که به صورت تصادفی توسط سایت‌های اینترنتی ایجاد شده‌اند) به‌راحتی دست پیدا کنند. در عین حال آنها می‌توانند از سیم‌کارت‌های دزدی یا یک بار مصرف (که بعد از انجام عمل کلاه‌برداری فیشینگ، خاموش می‌شود.) هم برای ارسال پیامک‌های فیشینگ به مشتریان بانک‌ها استفاده کنند. در همه این موارد شما پیامی دریافت می‌کنید که ظاهرا از سوی بانک شماست؛ ولی در واقع دامی است که برای کلاه‌برداری فیشینگ از شما پهن شده است. یک بانک هیچ‌وقت جز از سرشماره‌ای که در آن نام بانک ذکر شده یا از نشانی ایمیلی به غیر از دامنه اصلی سایت بانک، برای شما پیامی نمی‌فرستد. کارمندان بانک هم به هیچ عنوان حق چنین کاری را ندارند. این‌ها نشانه‌هایی است که لازم است به آنها توجه کنید تا قربانی فیشینگ نشوید.

مجرمان چگونه عملیات فیشینگ را انجام می‌دهند؟

۱. مجرم مورد نظر برای شما از طریق پیامک یا ایمیل، پیامی ارسال می‌کند که اطلاعات بانکی شما در معرض خطر است و به همین دلیل، حساب بانکی شما غیرفعال یا تعلیق شده است. این پیام از شما می‌خواهد تا معتبربودن اطلاعات یا تراکنش‌های خود را تصدیق کنید؛ مثلا از طریق ارائه اطلاعاتی چون شماره کارت پرداخت، شماره ملی، رمز حساب بانکی یا اطلاعات کاملا خصوصی مانند نام پدر یا مادر شما. مجرم پشت این پیام، از ادبیات و لحنی استفاده می‌کند که به شما القا کند موضوع اشاره‌شده در پیام، موضوعی کاملا فوری است که امنیت و اعتبار حساب بانکی شما را تهدید می‌کند. مثلا ممکن است این پیام به شما بگوید: «اگر به‌سرعت به این پیام، پاسخ ندهید، حساب بانکی شما به‌زودی به صورت کامل بسته یا به صورت موقت تعلیق می‌شود.» یا «در صورت عدم پاسخ به این پیام، جریمه خواهید شد!»
۲. حتما شما بسیاری از این پیام‌ها را قبلا دیده‌اید و می‌توانید جعلی‌بودن آنها را

تشخیص دهید؛ اما برخی از این پیام‌ها آنچنان ماهرانه نوشته و ارسال می‌شوند که حتی حرفه‌ای‌ترین کاربران هم در مورد ارسال آنها توسط یک مرجع معتبر، شک نمی‌کنند. در هر حال باید همیشه به بخش «ارسال‌کننده» چه در مورد پیامک و چه در مورد ایمیل، توجه کنید. در اغلب اوقات با کمی دقت، از همین بخش، متوجه جعلی‌بودن پیام ارسالی می‌شوید؛ اما تنها توجه به این بخش کافی نیست، چون توسط مجرمان حرفه‌ای قابل دورزدن است.

۳. در اغلب مواقع، پیام‌های فیشینگ، احتمالا دارای غلط‌های املایی یا انشایی هستند. حتی ممکن است نشانی وب‌سایتی که در متن پیام از شما درخواست شده به آن مراجعه کنید هم شکل به‌هم‌ریخته یا به صورت غلط نوشته‌شده وب‌سایت بانک شما باشد تا شما را ترغیب کند وارد سایت جعلی مشابه سایت بانک خود شوید. پس حتما به غلط‌های این‌چنینی در متن پیام دریافتی حساس باشید.

۴. برخی از پیام‌های فیشینگ، به شما وعده یک جایزه یا هدیه معتبر را می‌دهند که پس از تکمیل یک پرسشنامه ساده یا پاسخ به چند سؤال ساده می‌توانید به آن دست پیدا کنید. مثلا در ایران، دریافت پین شارژ اپراتورها یا حجم اینترنت رایگان، وعده جعلی شایعی است که توسط فیشینگ‌کاران به مردم ناآگاه داده می‌شود. اما سؤالاتی که آنها برای هدیه‌دادن این جایزه از شما می‌پرسند، در واقع با هدف دریافت اطلاعات حساس و شخصی شما به منظور استفاده مجرمانه است.

۵. برخی دیگر از پیام‌های جعلی به گونه‌ای نوشته می‌شوند که گویی شغلی جذاب توسط یک شرکت معتبر به شما پیشنهاد شده است. این شغل‌های وعده‌داده‌شده جعلی معمولا به شکل «کار در منزل» یا «درآمد عالی با چند ساعت کار در روز» ارائه می‌شوند و شرایط و مزایای‌شان آنقدر جذاب است که نه تنها کارجویان، بلکه شاغلین را هم وسوسه می‌کنند! این پیام دروغین، حاوی لینک یک وب‌سایت جعلی است که به شکلی کاملا حرفه‌ای هم طراحی شده تا سایت یک شرکت واقعی به نظر برسد و حتی شما را به یاد سایت‌های شرکت‌های معروف بیندازد. بعد از مراجعه به سایت، مجرم فیشینگ از شما می‌خواهد تا برای استخدام‌شدن، اطلاعات شخصی خود را وارد کنید و مبلغ اندکی را هم به عنوان هزینه ثبت‌نام پرداخت؛ در حالی که در پشت پرده، مجرم، در حال جمع‌آوری اطلاعات شما برای استفاده غیرقانونی است.

نکاتی برای درامان‌ماندن از خطر حملات فیشینگ

۱. همیشه به خاطر داشته باشید که بانک یا کارمندان آن، هرگز برای شما پیامی نمی‌فرستند که از شما بخواهد اطلاعات محرمانه خود را ارائه دهید. اگر پیامک یا ایمیلی دریافت کردید که از شما می‌خواست اطلاعات حساس مربوط به امنیت حساب بانکی یا

کارت پرداخت (نظیر شماره حساب یا کارت، پین امنیتی یا رمز) خود را ارائه دهید، هرگز نباید به چنین پیامی پاسخی بدهید.

۲. در هر زمانی که به نشانی وب‌سایت درج‌شده در یک پیامک یا ایمیل مراجعه می‌کنید، مطمئن شوید که نشانی (URL) سایت، به صورت صحیح و بدون غلط نوشته شده باشد و با وب‌سایت بانک شما یا شبکه پرداخت کارتی شما (در ایران سایت شرکت شاپرک بانک مرکزی) مطابقت داشته باشد. به شما توصیه اکید می‌کنیم که همیشه نشانی سایت بانکتان را خودتان در مرورگرتان تایپ کنید یا آن را در مرورگر اینترنتتان ذخیره کنید تا در زمان نیاز، مطمئن باشید دارید به سایت اصلی بانک مراجعه می‌کنید. در غیر این صورت ممکن است متوجه جعلی‌بودن پیام دریافتی نشوید، روی لینک درج‌شده در متن پیام، کلیک کنید و اطلاعات شخصی‌تان را خودتان با دست خودتان در اختیار مجرم فیشینگ بگذارید.

۳. پیامک‌ها یا ایمیل‌های جعلی دریافت‌شده را اول به عنوان «اسپم (Spam)» نشانه‌گذاری کنید و بعد به‌سرعت پاک کنید. به صورت خاص درمورد ایمیل‌های دریافتی، به هیچ عنوان روی فایل‌های ضمیمه (Attachment) کلیک و آنها را دانلود نکنید؛ چراکه ممکن است آن فایل ضمیمه، آلوده به ویروس یا بدافزار دیگری باشد.

۴. اگر پیشنهاد جایزه، هدیه یا شغلی خیلی جذاب را از طریق پیامک یا ایمیل دریافت کردید، قبل از هر کاری، مطمئن شوید که آن پیام از منبعی معتبر ارسال شده است.

ب. کلاه‌برداری از طریق وب‌سایت‌های جعلی (اسپوفینگ = Spoofing)

اسپوفینگ عبارت است از ایجاد یک وب‌سایت، به عنوان طعمه‌ای برای به‌دام‌انداختن افراد ناآگاه به منظور انجام اعمال مجرمانه. برای اینکه سایت جعلی ایجادشده معتبر به نظر برسد، مجرمین معمولا وب‌سایت خود را به شکلی ماهرانه و به گونه‌ای طراحی می‌کنند که اسامی، لوگوها، طراحی گرافیکی و حتی عملکردهای آن مشابه سایت‌های واقعی به نظر برسد. آنها حتی تلاش می‌کنند تا حد امکان نشانی (URL) و آیکون سایت جعلی هم که در بالای مرورگرتان مشاهده می‌کنید، مشابه سایت‌های معتبر باشد.

مجرمان چگونه عملیات اسپوفینگ را انجام می‌دهند؟

مجرم مورد نظر برای شما از طریق پیامک یا ایمیل، لینکی را ارسال می‌کند که شما را به وب‌سایت جعلی ایجادشده توسط مجرم، ارجاع می‌دهد. پیام ارسالی از شما می‌خواهد که اطلاعات شخصی خود را در نشانی موجود در متن پیام، به‌روزرسانی یا تائید کنید؛ هر چند که هدف وی، دسترسی به اطلاعات محرمانه شما مانند نام کاربری اینترنت‌بانک، رمز عبور، پین امنیتی، شماره حساب بانکی یا کارت پرداخت شما، کد CVV کارت پرداخت شما و دیگر اطلاعات محرمانه‌ای از این دست است.


FRAUD

نکاتی برای درامان‌ماندن از خطر حملات اسپوفینگ

۱. همیشه به خاطر داشته باشید که بانک یا کارمندان آن، هرگز برای شما پیامی نمی‌فرستند که از شما بخواهند اطلاعات محرمانه خود را ارائه دهید. اگر پیامک یا ایمیلی دریافت کردید که از شما می‌خواست اطلاعات حساس مربوط به امنیت حساب بانکی یا کارت پرداخت مانند شماره حساب یا کارت، پین امنیتی یا رمز خود را ارائه دهید، هرگز نباید به چنین پیامی پاسخی بدهید.

۲. به دنبال آیکون تائیدیه اعتبار وب‌سایت (Padlock) بگردید: یک استاندارد رایج در مرورگرهای وب وجود دارد که وب‌سایت‌های معتبر را به گونه‌ای مشخص می‌کند. این آیکون به شکل یک قفل، در سمت چپ نوار آدرس در بالای مرورگر نمایش داده می‌شود که می‌توانید با کلیک روی آن از طریق موس رایانه یا لمس آن در صفحات نمایش لمسی، جزئیات اعتبارنامه امنیتی وب‌سایت مورد نظر را ببینید. اگر وب‌سایتی که به آن مراجعه کردید، دارای مشکل امنیتی باشد، معمولا اخطارهایی توسط خود مرورگر به شما نشان داده می‌شود. به این اخطارها توجه کنید و سریع از آن وب‌سایت، خارج شوید. ضمنا بعضی از وب‌سایت‌های جعلی، آیکونی مشابه آیکون Padlock را در نوار آدرس مرورگر به شما نشان می‌دهند که با کلیک روی آن و بازنشدن منوی امنیتی، می‌توانید از جعلی‌بودن آن مطمئن شوید.

۳. همیشه نشانی (URL) وب‌سایتی را که به آن مراجعه کرده‌اید، به صورت دقیق بررسی کنید. سایت‌های معتبر از جمله سایت‌های بانک‌ها در ابتدای نشانی‌شان عبارت «https://:» را دارند (که معنای آن، امن‌بودن ارتباط میان دستگاه شما با سرور آن وب‌سایت است.) اگر در ابتدای نشانی وب‌سایتی که شبیه سایت بانک شماست عبارت «http://:»وجود دارد، (به تفاوت "s" در این عبارت با عبارت خط بالاتر توجه کنید.) آن سایت حتما جعلی است. به عنوان مثال نشانی صحیح اینترنت‌بانک پاسارگاد عبارت است از: https://ib.bpi.ir. هر نشانی دیگری غیر از این نشانی، یک وب‌سایت جعلی است که به بانک پاسارگاد ارتباطی ندارد.

انواع تخلف و تقلب در حوزه تلفن‌بانک

فیشینگ از طریق تلفن (ویشینگ=Vishing)

ویشینگ ترکیبی است از تماس تلفنی و فیشینگ که معمولا از طریق شماره‌های تلفن اینترنتی (VoIP) انجام می‌شود. در این روش، مجرم، خودش را طی یک تماس تلفنی به جای کارشناس مرکز تماس بانک، جا می‌زند تا با فریب مشتریان ناآگاه، اطلاعات شخصی و مالی آنها را از طریق تلفن، برای مقاصد مجرمانه خود، دریافت کند.

مجرمان چگونه عملیات ویشینگ را انجام می‌دهند؟

یک نوع رایج از حملات ویشینگ می‌تواند به شکل فرایند زیر اتفاق بیفتد:

۱. مجرم از طریق ابزارهای تلفن اینترنتی، یک تلفن گویای جعلی را ایجاد می‌کند و سپس به صورت تصادفی شروع به تماس‌گرفتن با شماره‌های تلفن مختلف مربوط به حوزه جغرافیایی مورد نظر خود مثلا ایران می‌کند.

۲. وقتی قربانی، تلفن خودش را پاسخ می‌دهد، یک پیام ضبط‌شده می‌شنود که به وی به عنوان مشتری بانک، اخطار می‌دهد با کارت بانکی وی، عملیات مجرمانه‌ای انجام شده و مشتری باید با گذراندن یک فرایند تائید هویت از طریق همین تماس تلفنی، این مشکل را حل کند. معمولا در ادامه از مشتری خواسته می‌شود تا پشت خط بماند یا کلیدی را روی تلفن خود فشار دهد تا فرایند آغاز شود یا اینکه در سریع‌ترین زمان ممکن با شماره تلفن اینترنتی جعلی که در همان پیام ضبط‌شده به مشتری اعلام می‌شود، تماس بگیرد.

۳. وقتی مشتری آغاز فرایند تائید هویت را انتخاب می‌کند، یک صدای مصنوعی ایجادشده توسط رایانه یا یک انسان واقعی، به او می‌گوید که بانک مشتری با وی برای «تائید هویت حساب بانکی» تماس گرفته و مشتری باید با گوش‌دادن به راهنمایی‌هایی که به وی اعلام می‌شود، اطلاعات هویتی یا مالی مورد نیاز را از طریق گوشی تلفن خود، وارد سیستم بانک کند. مجرم ویشینگ، به احتمال زیاد هیچ چیزی درمورد قربانی خود نمی‌داند و به او «جناب آقا» یا «سرکار خانم» می‌گوید؛ در حالی که مرکز تماس بانک، حتما نام مشتری را در تماس تلفنی به مشتری اعلام می‌کند.

۴. مجرم ویشینگ، طی این تماس تلفنی، اطلاعات حساسی چون شماره کارت پرداخت، رمز و تاریخ انقضای آن، تاریخ تولد، شماره حساب بانکی و مانند آنها را از خود مشتری به دست می‌آورد.

۵. زمانی که قربانی، اطلاعات درخواست‌شده را به مجرم ویشینگ، ارائه داد، مجرم، هر آن چیزی را که برای عمل مجرمانه خود به آن نیاز دارد، در اختیار خواهد داشت.

نکاتی برای درامان‌ماندن از خطر حملات ویشینگ

۱. توجه داشته باشید که وقتی بانک با شما تماس می‌گیرد، حتما حداقل اطلاعاتی درمورد شما دارد؛ از جمله نام و نام خانوادگی شما! بنابراین به هر تماس‌گیرنده تلفنی که ساده‌ترین اطلاعات شخصی (نام و نام خانوادگی) را درمورد شما نمی‌داند، شک کنید. (هر چند حتی همین عامل هم لزوما به‌تنهایی کافی نیست.) اگر چنین تماسی دریافت کردید، آن را سریع به مرکز تماس بانک خود گزارش کنید.

۲. به هیچ عنوان به هیچ شماره تلفنی که از طریق تلفن، پیامک یا ایمیل از شما درخواست تماس برای حل مشکل امنیتی کارت پرداخت یا حساب بانکی را دارد، زنگ نزنید. اطلاعات

شخصی و بانکی خود را در هیچ سامانه تلفنی که به محض تماس با شما برای شما یک پیام ضبط‌شده را پخش می‌کند، وارد نکنید.
۳. وقتی چنین تماسی را دریافت کردید، اولین کاری که باید بکنید تماس با شماره تلفن مرکز تماس بانکتان است که روی کارت بانکی یا دفترچه حساب بانکی شما نوشته شده یا در سایت خود بانکتان درج شده است. بدین ترتیب می‌توانید مطمئن شوید که تماس را از خود بانک دریافت کرده‌اید و در غیر این صورت، گزارش تماس جعلی را به بانک بدهید تا آنها موضوع را از مراجع قضایی و امنیتی پیگیری کنند.

انواع تخلف و تقلب در حوزه کارت‌های پرداخت

الف. دزدیدن کارت پرداخت یا اطلاعات آن (اسکیمینگ = Skimming)

اسکیمینگ روشی است که توسط مجرمان برای دسترسی به اطلاعات کارت پرداخت مشتریان استفاده می‌شود تا بتوانند از این اطلاعات برای تراکنش‌های مجرمانه خود استفاده کنند.
روش کار مجرمین برای اسکیمینگ معمولا استفاده از دستگاهی به نام «اسکیمر (Skimmer)» برای کپی‌کردن اطلاعات ذخیره‌شده روی نوار مغناطیسی کارت شماست. اطلاعات کارت کپی‌شده یا روی همان دستگاه ذخیره می‌شود یا اینکه به یک رایانه منتقل می‌شود تا بعدا برای عملیات مجرمانه از آن بهره‌برداری شود.

نکاتی برای درامان‌ماندن از خطر حملات اسکیمینگ

۱. **هشیار باشید:** همیشه در زمان انجام پرداخت‌های کارتی حضوری (خرید از طریق دستگاه کارت‌خوان)، مواظب باشید که کارتتان در جلوی چشم خودتان باشد و در دستگاهی به غیر از دستگاه کارت‌خوان، کشیده نشود.
۲. **از رمز کارتتان محافظت کنید:** سعی کنید حتما رمزتان را خودتان در دستگاه کارت‌خوان (یا خودپرداز یا همان ATM) وارد کنید و در زمان واردکردن هم حواستان باشد تا افراد حاضر در اطراف شما رمزتان را متوجه نشوند.
۳. **همیشه رسیدهای خرید خود را بررسی کنید:** مطمئن شوید که مبلغ، تاریخ و زمان خرید در آنها به‌درستی درج شده است.
۴. **گردش حساب بانکی یا کارت خود را به صورت منظم، بررسی کنید:** هر گونه تراکنش غیرمجاز را در سریع‌ترین زمان ممکن به بانک خود گزارش دهید.

ب. تقلب‌های پنهان‌شده در بازاریابی اینترنتی (تله‌مارکتینگ = Telemarketing) برای ارائه پیشنهادهای خرید و تخفیفات

بسیاری از شرکت‌ها ممکن است در طول زمان، تصمیم بگیرند پیشنهادات جذاب

خرید (پروموشن) را به مشتریان بالقوه خود ارائه دهند که نوعی خرید مجانی هم به حساب می‌آیند. در دنیای امروز در بسیاری موارد، این پیشنهادات به صورت آنلاین به افراد ارائه می‌شوند. چیزی که بسیاری از افراد متوجه آن نیستند این است که در زمان درخواست دریافت آن پیشنهاد یا تخفیف خرید، با پذیرش شرایط پنهان‌شده در پشت صحنه توافق‌نامه دریافت آن، به شرکت ارائه‌کننده اجازه می‌دهند که در آینده همچنان آن خدمت را برای مشتری فعال نگه دارد و بابت این فعال نگه‌داشتن هم مشتری را به صورت موردی یا دوره‌ای (مثلا ماهانه) شارژ کند. (به عنوان مثال به کدهای تخفیف خرید اشتراک کسب‌وکارهای آنلاین توجه کنید.) این هزینه‌های پنهان‌شده که به صورت خودکار هم از کارت افراد فریب‌خورده برداشت می‌شوند، در زمان برداشت وجه، باعث تعجب و نگرانی آنها می‌شوند.

نکاتی برای درامان‌ماندن از خطر تقلب‌های پنهان‌شده در بازاریابی اینترنتی

۱. مطمئن شوید که در زمان پذیرش توافق‌نامه خرید در قالب پیشنهاد یا تخفیف، حتما شرایط آن را به‌دقت مطالعه کرده‌اید و از تمام حقوق درخواست‌شده توسط فروشنده به‌خوبی آگاه شده‌اید و سپس آن را پذیرفته‌اید.

۲. تکلیفتان را خودتان انجام دهید. بدون آگاهی کامل از قانونی‌بودن و معتبربودن درخواست‌های فروشنده برای ارائه پیشنهاد خرید ویژه یا تخفیف، به هیچ عنوان اقدام به سرمایه‌گذاری یا خرید یک محصول یا خدمت نکنید. اطلاعات کارت یا حساب بانکی خود را به محض دریافت یک پیشنهاد جذاب، بدون بررسی دقیق، در اختیار فروشندگان نگذارید.

۳. اگر قبل از پرداخت وجه، متوجه شدید که پیشنهاد ارائه‌شده شامل شرایطی است که هزینه‌های اضافی و غیرقابل قبولی را به شما تحمیل می‌کند، به‌سرعت با فروشنده تماس بگیرید و از او بخواهید تا خرید شما را لغو کند. اگر بعد از پرداخت وجه متوجه این موضوع شدید، به‌سرعت با بانک خود تماس بگیرید.

ج. دزدیده‌شدن یا گم‌شدن جسم کارت و انجام تراکنش‌های غیرمجاز با آن

واقعیت ناخوشایند این است که ممکن است به هر دلیلی شما کارت پرداخت خود را گم کنید، آن را جا بگذارید یا اینکه کارتتان را از شما بدزدند. احتمال دارد در این حالت از کارت شما برای تراکنش‌های غیرمجاز استفاده شود. این تراکنش‌های غیرمجاز می‌تواند در قالب برداشت از خودپرداز، خرید از کارت‌خوان یا خرید آنلاین رخ بدهند.

گام‌هایی که باید پس از اینکه متوجه دزدیده‌شدن یا گم‌شدن کارت خود شدید، انجام دهید:

۱. به‌سرعت با مرکز تماس بانک خود تماس بگیرید یا اینکه به نزدیک‌ترین شعبه بانک

مراجعه کنید تا گزارش دزدیده‌شدن یا مفقودشدن کارت خود را ارائه بدهید.
۲. حساب بانکی خود را بررسی کنید تا متوجه شوید آیا هیچ گونه تراکنش غیرمجازی انجام شده است یا نه. اگر تراکنش غیرمجازی را دیدید، سریع به بانک خود اطلاع دهید.

نکاتی برای درامان‌ماندن از خطر تراکنش‌های مجازِ ناشی از دزدیده‌شدن یا گم شدن کارت خود

۱. به هیچ عنوان رمز کارت خود را روی جسم کارت ننویسید.
۲. همیشه در زمان ورود رمز کارت خود روی خودپرداز یا دستگاه کارت‌خوان، مراقب باشید تا افراد دور و اطراف شما نتوانند رمز واردشده شما را متوجه شوند.
۳. همیشه مراقب اطراف خود باشید.
۴. رمز مشترکی برای تمامی کارت‌های پرداخت خود تنظیم نکنید.

انواع تخلف و تقلب در حوزه چک

هر گونه تخلف و تقلب در حوزه چک، جرم محسوب می‌شود که شامل فریب‌دادن افراد یا کسب‌وکارها در زمان خرید از آنها از طریق چک، برات یا سفته می‌شود.

هنوز معاملات بسیار زیادی در قالب پرداخت از طریق چک انجام می‌شوند. متأسفانه در برخی موارد، تازه در زمان گذاشتن چک به حساب بانکی برای دریافت وجه است که مشخص می‌شود چک مربوطه دچار یک مشکل مجرمانه (مثلا جعلی بودن یا دزدی بودن) است؛ آن هم در حالی که فرد دریافت‌کننده وجه از طریق چک، هیچ اطلاعی از موضوع نداشته است.

دو نوع اصلی از تقلب و تخلف‌های مربوط به چک عبارتند از:

• جعل چک: چکی که از روی یک چک واقعی بانکی کپی‌برداری شده یا به شکلی طراحی شده که واقعی به نظر برسد.

• دستکاری چک: در این حالت، چک، واقعی است؛ اما به صورت غیرمجاز، دستکاری و مخدوش شده تا عدد پرداختی که مغایر با نظر صادرکننده چک است، در آن درج شود.

نکاتی برای درامان ماندن از خطر تخلف و تقلب‌های مربوط به چک

۱. به هیچ عنوان چک‌های صادرشده توسط افراد دیگری غیر از طرف معامله خود را که نمی‌شناسید، قبول نکنید.

۲. اگر چک ارائه‌شده توسط خریدار، دچار آسیب ظاهری مشهودی شده یا حدس می‌زنید چک، دستکاری شده باشد، از خریدار، درخواست یک چک جدید کنید.

۳. اگر متوجه شدید که چک دریافت‌شده دچار نوعی تخلف و تقلب است و آن را به حساب خود خوابانده‌اید، موضوع را به‌سرعت به بانک خود اطلاع دهید.

کلاه‌برداری‌های مرتبط با چک (Scams)

بسیاری از افراد ناخواسته قربانی تخلف و تقلب مرتبط با چک می‌شوند. این کلاه‌برداری‌ها معمولا به این شکل رخ می‌دهند؛ کلاه‌بردار به سراغ قربانی می‌رود و او را به هر روشی راضی می‌کند تا فعالیت‌هایی انجام دهد که حساب بانکی وی را تحت خطر قرار می‌دهد. مثلا به پدیده حساب‌های اجاره‌ای در اقتصاد ایران توجه کنید.

نمونه ماجرایی که اتفاق می‌افتد به این شکل است: کلاه‌بردار، در برابر وعده یک مبلغ وسوسه‌انگیز، یک چک مشکل‌دار را در اختیار قربانی قرار می‌دهد و قربانی را برای خواباندن چک به حساب خود و برداشت وجه آن راهنمایی می‌کند. (تحصیل مجرمانه چک.) وقتی مشکل‌داربودن چک معلوم شد، در صورتی که مبلغ چک از حساب بانکی قربانی برداشت یا جابه‌جا شده باشد، صاحب حساب در برابر جرم مربوط به چک، مسئولیت قانونی پیدا می‌کند؛ در حالی که کلاه‌بردار هم ناپدید شده است.

نکاتی برای درامان‌ماندن از خطر کلاه‌برداری‌های مرتبط با چک

۱. به هیچ عنوان و تحت هیچ شرایطی عملیات مربوط به دریافت و پرداخت وجوه بانکی را از طرف کارفرما یا شرکت محل کار خود انجام ندهید.
۲. در زمان دریافت وجه از طریق چک، در برابر اضافه واریزها یا درخواست بازگشت وجه هشیار باشید.
۳. هویت و اعتبار مالی پرداخت‌کننده وجه از طریق چک را با دقت بررسی کنید. مثلا در ایران می‌توانید از طریق سامانه صیاد بانک مرکزی وضعیت اعتبار صادرکننده چک را استعلام کنید.

دزدیده‌شدن هویت قانونی

وقتی یک مجرم بدون اطلاع یا رضایت شما از اطلاعات شخصی و هویت قانونی شما مانند نام، کد ملی، شماره کارت، شماره تلفن همراه و مانند آنها استفاده کند، شما قربانی دزدی هویت قانونی شده‌اید.

نکاتی برای درامان‌ماندن از خطر دزدیده‌شدن هویت قانونی

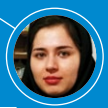
• در حفظ اطلاعات شخصی، هویتی و قانونی خود کاملا بکوشید.
• تحت هیچ شرایطی اطلاعات شخصی خود را از طریق تلفن، ایمیل یا اینترنت در اختیار دیگران قرار ندهید، مگر اینکه خودتان فرایند ارائه اطلاعات را با اطمینان از واقعی‌بودن آن شروع کرده باشید یا اینکه درخواست‌کننده اطلاعات را کاملا بشناسید.
• هیچ یک از رمزهای خود (رمز کارت، اینترنت‌بانک و...) را در اختیار هیچ فردی قرار ندهید.
• کپی فیزیکی تمامی مدارک هویتی و مستندات حاوی اطلاعات شخصی پس از استفاده باید به روشی مطمئن (مثلا خردکردن کاغذ) از بین برده شوند.
• از رمزهای بسیار قوی استفاده کنید و آنها را به صورت دوره‌ای به‌روزرسانی کنید.
• گزارش اعتبارسنجی خود را حداقل سالی یک بار بررسی کنید. در ایران این گزارش توسط شرکت رتبه‌بندی اعتباری ایرانیان تحت نظر بانک مرکزی صادر می‌شود.

منبع:

https://www.icicibank.ca/en/safebanking/bewarefrauds

گفت‌وگو با فاطمه سلطانی مدیر پروژه سامانه کشف تقلب داتین

شناسایی تراکنش‌های مشکوک را از قمار شروع کردیم



فاطمه قوتی

داده‌های افراد در حوزه بانکی و پرداخت، آنقدر گسترش یافته که بروز تقلب و تخلف در آنها امری غیر قابل اجتناب به نظر می‌رسد. در این میان، همان‌طور که هر روز اهمیت این داده‌ها در زندگی افراد افزایش پیدا می‌کند، تلاش نهادهای مالی این بوده که وقوع این مسائل را به حداقل برسانند. پیش‌تر روش‌های کشف تقلب آفلاین یا همان کلاسیک، بهترین راهکار بود اما حالا با حضور و ظهور هر چه پررنگ‌تر تکنولوژی، به نظر می‌رسد شیوه‌های آنلاین بهتر از گذشته بتوانند از عهده تشخیص صحت این تراکنش‌ها برآیند.
شرکت داتین با توجه به ارائه راهکارهای جامع بانکی از چند سال گذشته، روش کشف تقلب آفلاین را در سبد محصولات خود داشته و حالا تمرکز بیشتری را روی سامانه کشف تقلب و تخلف آنلاین خود گذاشته است. سامانه‌ای که به گفته مدیرانش، بر اساس جدیدترین تحقیقات و مطالعات در این حوزه طراحی شده است.
این گفت‌وگو درباره این سامانه و ویژگی‌های آن است و مدیر پروژه سامانه کشف تقلب

داتین درباره امکان پیاده‌سازی آن و تاثیراتی که در نظام بانکی کشور دارد، صحبت کرده است.
فاطمه سلطانی، مدیر پروژه سامانه کشف تقلب داتین درباره راه‌اندازی سامانه کشف تقلب این شرکت گفت: «برای اینکه سامانه کشف تقلب آنلاین داتین را به بهره‌برداری نهایی برسانیم، چندین مرحله تست و بررسی داشتیم و در هر مرحله اصلاحات لازم ایجاد شد تا زیرساختی قوی، سریع و دقیق برای بانک‌ها ایجاد کنیم. به طور کلی با توجه به مدل‌های مختلف تخلف و تقلب، ما در ابتدا مسائل اجتماعی را شناسایی کردیم و به این نتیجه رسیدیم که سرقت و کپی کارت بیشتر است و قطعا از این طریق، تراکنش‌های مشکوک ما افزایش پیدا می‌کند. همچنین تراکنش‌های قمار یکی از موارد پر تواتر است و به همین دلیل از قمار شروع کردیم. خوشبختانه ۱۰۰ درصد مواردی که شناسایی و ریجکت کردیم، درست بود و در هیچ کدام هم تشخیص غلط نداشتیم.»

سلطانی درباره چگونگی کشف تقلب یا تخلف در این سامانه گفت: «ما از طریق این سامانه، تراکنش را در صف قرار می‌دهیم تا دیتا پردازش شود. این زمان، معمولا زیر ۵۰ میلی ثانیه است. البته در زمان پربازی ممکن است بعضی از این تراکنش‌ها از کنترل ما خارج شود، به همین دلیل عدد ۱۰۰ میلی ثانیه را انتخاب کردیم.»

مدیر پروژه سامانه کشف تقلب داتین، در ادامه گفت: «بانک‌ها برای گرفتن این سرویس، باید بتوانند اطلاعات لازم را از شرکت ارائه‌دهنده کربنکینگ خود به طور سیستماتیک اخذ کنند. مسئله دیگر، سیستم و سخت‌افزاری است که بانک‌ها به آن نیاز دارند چراکه پرفورمنس باید بسیار بالا باشد. در این زمینه باید تاکید کنم تمام تولیدات داتین بر اساس بررسی جدیدترین تحقیقات و مطالعات در حوزه تقلب و درنظرگرفتن شرایط موجود طراحی شده است.»

سلطانی درباره پیاده‌سازی این سامانه گفت: «ما سناریویی که بتوانیم چطور از کاربر، مشتری و بانک در زمان ثبت تراکنش مشکوک بازخورد بگیریم، آماده کرده‌ایم و این محصول، آماده پایلوت شدن روی یکی از مشتریان است.»

او در پاسخ به این سوال که آیا داتین می‌تواند این سیستم را برای بانک مرکزی بنویسد و بانک مرکزی به تمام بانک‌ها ارائه دهد، گفت: «بله، توانایی پیاده‌سازی این سامانه توسط داتین وجود دارد، چراکه طرح‌های ما بسیار کامل و این سیستم، جنبه‌های مختلف اجتماعی، کارفرمایی و رگولاتوری را در نظر گرفته است. با توجه به اینکه یکی از مهم‌ترین موضوعات برای بانک‌ها جذب و حفظ منابع است، جلوگیری از مواردی که با روش‌های تخلف یا تقلب منجر به آسیب به دارایی مشتریان و خروج منابع یا لطمه به شهرت بانک می‌شوند، بسیار حائز اهمیت است. از سوی دیگر، در جنبه اجتماعی، اعتمادی به بانک‌ها وجود دارد که این سامانه، آنها را در حفظ و ارتقای آن یاری می‌دهد.»

او در پاسخ به این سوال که داتین تاکنون چند نسل از سامانه‌های کشف تقلب خود را ارائه داده و این سامانه‌ها چه تفاوت‌هایی با یکدیگر دارند، گفت: «نسل اول، سامانه نظارتی است که به صورت آفلاین، در پایان هر روز بر اساس داده‌های جمع‌آوری‌شده از سامانه‌های بانکی، پردازش اطلاعات را انجام داده و در ابتدای روز بعد گزارش‌های متنوعی را در ده‌ها موضوع مختلف که مشکوک شناسایی شده‌اند، ارائه می‌دهد. نسل دوم این سامانه‌ها نیز سامانه آنلاین ماست.»

سلطانی در پایان درباره معماری زیرساخت این سامانه گفت: «در این سامانه با توجه به حجم ورودی تراکنش هر بانک، زمان بررسی و تحلیل تراکنش به صورت آنلاین و قبل از ورود به دیتابیس‌های بانکی بدون ایجاد اخلال در تراکنش‌ها، وجود دارد. همچنین با وجود طراحی به صورت سه لایه‌ای (آنلاین، آفلاین و near online) امکان بررسی در سطوح مختلف با تکنولوژی‌های متعدد امکان‌پذیر است.»

تقلب و کشف تقلب، رقابتی نزدیک

محمد رحمتی و کیمیا قاسم‌زاده
کارشناس راهکارهای کشف تقلب داتین

با ورود تکنولوژی به صنایع گوناگون، سازوکار ارائه خدمات در صنایع، با تغییرات بسیاری همراه شده است. در این میان، صنعت بانکداری نیز از این قاعده مستثنی نبوده و بانکداری مدرن تغییرات چشم‌گیری را نسبت به بانکداری سنتی مشاهده کرده است. به عنوان مثال می‌توان به انواع خدمات جدید بانکداری اینترنتی، خدمات مبتنی بر USSD، همراه‌بانک و... اشاره کرد. اما رشد سریع تکنولوژی به طور معمول سبب می‌شود رواج خدمات جدید، بر یادگیری طریقه صحیح استفاده از آنها پیشی بگیرد و این اتفاق در برخی از صنایع از جمله صنعت بانکداری، نقطه ورود سوءاستفاده‌کنندگان و کلاه‌برداران است. در سمت دیگر، متخصصان نیز در تلاشند تا با ایمن‌سازی سازوکارهای استفاده از خدمات، احتمال وقوع کلاه‌برداری را به حداقل برسانند. دلیل این است که کاهش نرخ تقلب علاوه بر افزایش اعتماد مشتریان و به تبع آن افزایش منابع بانک، باعث خواهد شد هزینه‌های عملیاتی بانک‌ها کاهش یابد که این موضوع بر خدمات‌رسانی بانک‌ها و

2.The rule-based Protection

موسسات مالی اثر خواهد داشت. این رقابت، رقابتی میان تقلب و کشف تقلب است.
به طور کلی، کشف تقلب به مجموعه فعالیت‌هایی گفته می‌شود که منجر به کاهش ریسک خروج غیر مجاز پول و کشف و پیشگیری از تخلف‌های بانکی یا جرائمی مانند پولشویی خواهد شد. تقلب‌های بانکی را می‌توان به طور کلی به موارد گوناگونی تقسیم کرد که از این جمله، تقلب‌های ناشی از حساب‌سازی[۱]، تقلب‌های مرتبط با وام‌های بانکی[۲]، تقلب‌هایی که از طریق وب اتفاق می‌افتد، فیشینگ[۳]، تراکنش‌هایی که در ظاهر به نفع بانک است ولی در اصل صرفا برای کلاه‌برداری از بانک هستند[۴]، تقلب از طریق خودپرداز[۵]، پولشویی[۶]، شرط‌بندی[۷] و تقلب در تراکنش‌های کارت[۸] برخی از رایج‌ترین آنهاست.
از آنجا که بیشترین سهم تبادلات مالی از طریق کارت‌های بانکی صورت می‌پذیرد، درصد بیشتری از پژوهش‌های انجام‌شده بر این نوع از تقلب تاکید داشته‌اند. انواع تقلب در حوزه کارت را می‌توان به دسته‌های زیر بخش‌بندی کرد:

۱- تقلب بدون حضور صاحب کارت و کارت (CNP):[۹]

این اصطلاح به نوعی از تقلب اطلاق می‌شود که در آن نیازی به حضور فیزیکی شخص یا وجود فیزیکی کارت نیست. برای مثال می‌توان از خریدهای آنلاین نام برد. سرقت اطلاعات حساب و سپس خرید اینترنتی با استفاده از اطلاعات سرقت‌شده، روشی رایج در سرقت از حساب بوده و هست.

۲ - دردست‌گرفتن کنترل حساب:[۱۰]

در این نوع از تقلب، سارق بعد از به‌دست‌آوردن اطلاعات شخص، رمز کارت را تغییر داده و از حساب فرد استفاده می‌کند.

۳ - کارت اسکیمینگ:[۱۱]

در این حالت، از دستگاه‌های اسکیمر که به یک دستگاه کارت‌خوان مانند خودپرداز یا پوز متصل می‌شود برای کپی‌کردن کارت استفاده می‌شود. سارق علاوه بر نیاز به داشتن کپی از کارت بانکی (که معمولا با گذاشتن چیپست‌های مشخص در دستگاه‌های پوز اتفاق می‌افتد) به گذرواژه نیز احتیاج دارد.

۴ - سرقت یا مفقودی کارت:[۱۲]

در این نوع تقلب، پس از صدور کارت‌های بانکی و عدم نیاز افراد به مراجعه فیزیکی به شعبه برای دریافت وجه نقد، سارقان به شیوه سنتی تلاش بر سرقت اصل کارت بانکی دارند. سارقان، گذرواژه واردشده توسط کاربران را در دستگاه های خودپرداز دیده و با سرقت اصل کارت، از آن برداشت می‌کنند.

1.Accounting fraud
2.Loan fraud
3.Phishing fraud
4.Rogue traders
5.ATM fraud
6.Money laundering
7.Gambling
8.Credit card fraud
9.Card-not-present fraud
10.Account take over
11.Credit card skimming
12.Lost and stolen credit card

از سایر روش‌های کلاه‌برداری می‌توان به vishing[۱۳]، Hijacking و Malware اشاره کرد. در Vishing کلاه‌بردار تلاش می‌کند تا با جلب اعتماد کاربر (با جعل عنوان شغلی مانند کارمند بانک و با ارائه اطلاعاتی که از سایر پایگاه‌های داده سرقت شده‌اند مانند کد ملی، نام پدر، آدرس دقیق محل سکونت و...) از کاربر اطلاعات حسابش را دریافت کند.
در این نوع، کلاه‌بردار با روش‌های گوناگون مانند ایجاد نگرانی و با بیان جملاتی از قبیل این حساب مسدود شده، از کاربر می‌خواهد کدی که برای او پیامک شده را به منظور رفع مسدودی، برای کلاه‌بردار ارسال کند. در Hijacking کلاه‌بردار تلاش می‌کند کنترل سیستم کاربر را به دست بگیرد. این نوع از کلاه‌برداری معمولا بر بستر اینترنت‌های نامعتبر یا سیستم‌های ناایمن رخ خواهد داد. معمولا کاربران می‌توانند با فعال‌کردن تنظیمات امنیتی سیستم‌های شخصی مانند firewall از این حملات در امان بمانند.
Malware‌ها نیز بدافزارهایی هستند که با اهداف مختلفی تولید می‌شوند. یکی از اهداف آنها دردست‌گرفتن کنترل سیستم کاربر در زمان تبادلات مالی است. یکی از نمونه‌های آن، بدافزاری با همین کاربری بود که مدتی با نام LFG-Malware شناخته می‌شد. از آنجایی که این بدافزار در اکثر مواقع غیرفعال است، توسط بسیاری از ایمن‌افزارها تشخیص داده نمی‌شد. این بدافزار با مکانیزم مشخصی در زمان ورود کاربران به یک صفحه پرداخت فعال شده و پس از ورود تمام اطلاعات توسط کاربر، پرداخت را متوقف کرده و خود از اطلاعات حساب کاربر استفاده می‌کرد. علاوه بر آن با نمایش پیغام جعلی و ساختگی از موفقیت‌آمیزبودن تراکنش، باعث عدم شک کاربران به سرقت در حال وقوع می‌شد.

رویکردهای کشف تقلب

۱- استفاده از قواعد از پیش تعیین‌شده

بانک‌ها و موسسات مالی تاکنون از رویکردهای مبتنی بر قاعده[۱۴] برای محدودکردن تراکنش‌های مشکوک و سپس بررسی این موارد به منظور تشخیص صحیح یا اشتباه‌بودن محدودیت ایجادشده استفاده کرده‌اند. این قوانین معمولا از طریق بررسی مواردی که تشخیص داده شده‌اند یا با استفاده از تجربیات کارشناسان خبره در این حوزه منتج شده‌اند. قابلیت توضیح و توجیه‌پذیری علت تقلب، شناخته‌شدن یک تراکنش و امکان پیاده‌سازی بدون نیاز به جمع‌آوری داده برای آموزش، از مزایای این روش‌ها هستند.
اگرچه نتایج این سیستم‌ها به میزان مناسبی قابل قبول است، اما افزایش متدهای تقلب در حوزه بانکی باعث شده که صرف استفاده از قواعد معین که انعطاف‌پذیری کمتری نسبت به روش‌های دیگر دارند، همیشه بهترین انتخاب نباشد. از معایب دیگر این روش نیز می‌توان به کشف الگوهایی از تقلب که پیچیدگی کمتری دارند اشاره کرد.

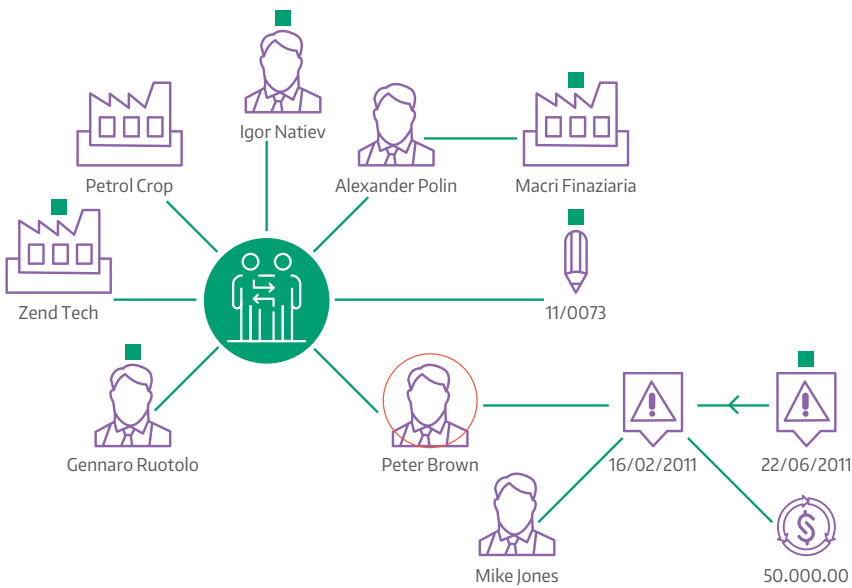
13.vishing 14.Rule-based


Username
****
Forgot Password?
Remember Me
LOGIN
REGISTER


15%
19%
38%
67%
89%

۲- استفاده از روش‌های یادگیری ماشین

مدل‌های یادگیری ماشین محدودیت‌های متدهای قاعده‌مند را مخصوصا در مواردی که ابعاد و ویژگی‌های داده زیاد باشد، تا حد قابل قبولی بهبود بخشیده‌اند. الگوریتم‌های کلاسیک یادگیری ماشین مانند درخت تصمیم، جنگل تصادفی، گرادیانت بوستینگ یا شبکه‌های یادگیری عمیق به همین منظور پیاده‌سازی می‌شوند. تشخیص الگوهای غیر خطی به صورت اتوماتیک و با استفاده از تعداد ویژگی‌های بالا (در صورت داشتن تعداد بالا) در مجموعه داده[۱۵] از شاخصه‌های این مدل‌هاست. نقطه قوت قابل توجه دیگر این است که امکان کشف الگوهای جدید تقلب با به‌روزرسانی مجموعه داده وجود دارد و برخلاف روش قاعده‌مند، نیازی به مهندسی معکوس روش‌های تقلب وجود ندارد. در کنار مزیت‌های گفته‌شده، مواردی همچون نیاز به وجود مجموعه داده برچسب‌خورده کافی برای شروع، عدم امکان توجیه علت تقلب و نامیزان‌بودن تعداد تراکنش‌های متقلبانه نسبت به تراکنش‌های عادی نیز برخی از چالش‌های پیش روی توسعه این مدل‌ها هستند. البته لازم به ذکر است که چالش نیاز به داده کافی برچسب‌خورده یکی از نیازمندی‌های مدل‌های بانظارت است که ممکن است یادگیری نیمه نظارتی یا بدون نظارت در مواردی باعث رفع چالش اشاره‌شده شوند.



بسیاری از ابزارهای کشف تقلب موجود، ترکیبی از الگوریتم‌های یادگیری ماشین و سیستم‌های قاعده‌مند را استفاده کرده‌اند که یکی از معایب آنها هزینه نگهداری بالاست. متدهای یادگیری عمیق نیز توجه زیادی را نسبت به موارد گفته‌شده به خود جلب کرده‌اند. در مدل‌های یادگیری عمیق به منظور کشف آنومالی، استفاده از مدل‌هایی با معماری خودرمزگذار متداول است. این روش‌ها نیز چالش‌هایی داشته و همیشه طبق انتظار پیش نرفته‌اند. همچنین به علت اهمیت مسیر گردش پول در برخی از سناریوهای تقلب، استفاده از شبکه‌های گراف یا ترکیب متدهای آنالیز گراف با یادگیری ماشین نیز بسیار مورد توجه است.

منبع:

1 -Deep learning for fraud detection in retail transactions. (2022). from https://medium.com/walmartglobaltech/deep-learning-for-fraud-detection-in-retail-transactions-564d31e5d1a3

2 - Machine Learning Models vs. Rule Based Systems in fraud prevention. (2022)., from https://nethone.com/post/machine-learning-models-vs-rule-based-systems-in-fraud-prevention

3 -Credit Card Fraud Detection Techniques - StaySafe.org. (2022), from https://staysafe.org/credit-card-fraud-detection-techniques/

4 - Digital Banking Fraud Detection Explained for Risk Executives | SEON. (2022), from https://seon.io/resources/banking-fraud-detection-and-prevention/

5 - Bajaj FinServ. (2022)., from https://www.bajajfinservmarkets.in/credit-card/credit-card-fraud.html

6 - Fraud Detection • Fraud Detection Machine Learning. (2022)., from https://perfectial.com/blog/fraud-detection-machine-learning/

7 - E-commerce Fraud Detection and Prevention: The In-depth Guide [Updated 2022] The Guide to eCommerce Fraud Detection & Prevention. (2022)., from https://spd.group/machine-learning/e-commerce-fraud-detection/

نگاهی به شکل فعالیت سامانه‌های کشف تقلب

سیدعلی طباطبایی
مدیر محصول راهکارهای مدیریت داده داتین

با پیشرفت‌های تکنولوژیک در حوزه بانکی و پرداخت، میزان تقلب و کلاه‌برداری‌های حرفه‌ای نیز افزایش پیدا کرده است. در این بین، با توجه به گسترش فعالیت‌های مالی و بانکی، فقدان یک سامانه جامع کشف تقلب در صنعت بانکی و پرداخت، معضلی با عنوان تراکنش‌های مشکوک را به وجود آورد. این موضوع باعث شد تا بسیاری از شرکت‌های فعال در اکوسیستم بانکی کشور، از جمله داتین طراحی و تولید چنین سامانه‌هایی را در دستور کار خود قرار دهند.

روش‌های کشف تقلب

۱. روش مبتنی بر قاعده (آفلاین):

در این روش، امکان تعریف یک یا چند قاعده بر اساس رفتار گذشته موجودیت دلخواه، وجود دارد. از این امکان، می‌توان برای شناخت موارد مشکوک یا مواردی که از نظر کاربر

نیاز به توجه بیشتر دارند، استفاده کرد. قواعد نیز می‌توانند از طرف نهادهای حاکمیتی یا رگولاتوری یا خبره‌های حوزه بانکی و پرداخت تعریف شوند.

۲. روش مبتنی بر هوش مصنوعی (آنلاین):
در برخی موارد رفتارهای متقلبانه به گونه‌ای صورت می‌گیرند که نمی‌توان قواعد دقیقی برای آنها پیاده‌سازی کرد. در چنین مواردی استفاده از روش‌های مبتنی بر قاعده کمکی به ما نمی‌کند و ناگزیر به استفاده از روش هوش مصنوعی با استفاده از مدل‌های یادگیری ماشین هستیم.
در این روش، مدلی بر اساس داده‌های تاریخی، داده‌های اخیر و انواع عوامل تاثیرگذار در روند رفتاری موجودیت‌های مختلف ایجاد می‌شود. این مدل، فاصله هر موجودیت از رفتار نرمال خودش و موجودیت‌های در خوشه خود را محاسبه می‌کند و به آنها برچسب ریسک اختصاص می‌دهد. در نهایت تصمیم می‌گیرد مواردی که بیشترین میزان ریسک را دارند، به عنوان مورد مشکوک به عنوان خروجی سامانه ارائه دهد.
در این روش، با استفاده از الگوریتم‌های خاص و همچنین پارالل کامپیوتینگ، زمان پاسخ‌دهی به زیر ۲۰ میلی‌ثانیه کاهش یافته که این سیستم می‌تواند با ترکیب دیگر زیرسیستم‌های بانک‌ها جلوگیری از تراکنش‌های مشکوک را اعمال کند.

فرصت‌های سامانه کشف تخلف و تقلب داتین و تاثیرات آن بر فعالیت بانکی

سامانه کشف تقلب در روش آفلاین براساس قواعد از پیش تعریف‌شده طراحی و پیاده‌سازی‌شده، می‌تواند کمک شایانی به متولیان این حوزه به ویژه اداره‌های بازرسی بانک‌ها بکند.
این سامانه با استفاده از زیرساخت انبارداده در تمامی ماژول‌ها و سامانه‌های بانکی، به صورت آفلاین موارد مشکوک را که با استفاده از ۱۳۰ قانون بررسی می‌شوند، تهیه و به بازرسان گزارش می‌کند. این امر باعث شد تا کار بازرسان که حدود سه روز طول می‌کشید به چهار ساعت کاهش پیدا کند.
همچنین در روش مبتنی بر هوش مصنوعی یا آنلاین، سامانه با استفاده از انبارداده و تکنولوژی کلان‌داده امکان توزیع‌پذیری و مقیاس‌پذیری حجم بالایی از داده‌های بانکی را فراهم کرده و همچنین می‌تواند مانع تراکنش‌های مشکوک شود.
ما در داتین با بررسی آخرین روش‌های پیشرفته و تکنولوژی‌های هوش مصنوعی همواره در حال به‌روزرسانی سامانه کشف تقلب هستیم. زیرساخت سامانه را نیز به گونه‌ای طراحی کردیم تا برای به‌روزکردن آن به کمترین زمان ممکن احتیاج داشته باشیم.

راهکارهای تشخیص تقلب

نیلوفر حق جو
کارشناس راهکارهای کشف تقلب داتین

آیا نیاز بشر به ثروت، نیازی طبیعی است؟ مکاتب بسیاری سعی در پاسخ به این سوال داشته‌اند و هر یک دلایل گوناگونی از جمله میل به قدرت، وجود سیستم‌های سرمایه‌داری، تامین نیازهای اولیه اساسی و... را علت ثروت‌طلبی بشر دانسته‌اند. هر چند لازمه پاسخ به این سوال، نیازمند بررسی و مکاشفه دقیق است اما آنچه به صورت حقیقتی غیر قابل انکار بین تمامی متفکران پذیرفته شده نیاز روزافزون بشر برای به‌دست‌آوردن هر چه بیشتر منابع مالی است.

بدیهی است که با ایجاد هر سیستم مالی، بسیاری از افراد با کشف خلا امنیتی سیستم، سعی در کسب منابع مالی با کمترین زحمت را دارند. در زمینه مبارزه با تقلب، دو نگاه کلی وجود دارد: اجتناب از تقلب و شناسایی آن[1] و طراحی سیستم‌هایی با امنیت بالا و برای مثال طراحی رمز دوم یا OTP که جزو طبقه اول این دسته‌بندی است. گاهی سیستم

امنیتی بسیار دقیق طراحی شده است؛ در این موارد متقلبین سعی می‌کنند با فریب افراد به مقاصد خود نائل شوند. از اینجا به بعد، سیستم‌های شناسایی تقلب برای جلوگیری از جابه‌جایی پول، کاربرد پیدا می‌کنند. یک موسسه تحقیقاتی در زمینه مالی[1] میزان کلاه برداری از طریق دزدی مشخصات در سال ۲۰۲۰ را حدود ۵۶ میلیون دلار تخمین زده است.[۲]

لازم به ذکر است که سیستم‌های کشف تقلب باید به طور مداوم، در طول زمان تکامل یابند، زیرا زمانی که دسته‌ای از تقلب‌ها کشف می‌شوند، استراتژی‌های قدیمی کنار گذاشته و با استراتژی‌های جدید تقلب جایگزین می‌شوند.

سیستم‌های کشف تقلب از الگوریتم‌های یادگیری ماشین، تحلیل‌های سری زمانی، تحلیل‌های آماری و ریاضیاتی و تحلیل گراف برای کشف تقلب استفاده می‌کنند. تقلب را می‌توان نوعی ناهنجاری در داده‌ها به حساب آورد؛ بنابراین می‌توان از این به بعد به جای اصطلاح کشف تقلب، شناسایی نمونه‌های ناهنجار را به کار برد. ناهنجاری‌ها در داده‌ها سه نوع مختلف دارند که لازم است در کشف هر تقلب دقت کنیم کدام یک از انواع ناهنجاری در حال رخ‌دادن است؛ در این صورت احتمال شناسایی خطا پایین می‌آید. این ناهنجاری‌ها عبارتند از:

• ناهنجاری‌های نقطه‌ای: زمانی که یک داده به صورت معناداری از بقیه داده‌ها متفاوت است. برای مثال، اگر موجودی یک کارت به صورت میانگین در هر روز برابر پنج هزار تومان باشد، موجودی برابر با پنج میلیارد تومان در یک روز تصادفی، ناهنجاری نقطه‌ای نامیده می‌شود.

• ناهنجاری‌های مبتنی بر زمینه: زمانی که یک داده با توجه به درنظرگرفتن شرایط موجود یا همان زمینه حضور، ناهنجار رفتار می‌کند. برای مثال، میزان برداشت از کارت در مواقع خاصی از سال مانند اسفند ماه (قبل از نوروز) افزایش می یابد. این افزایش برداشت در اسفند ماه رفتاری معمول است، در صورتی که همین افزایش برداشت در ماه‌های دیگر سال رفتاری ناهنجار محسوب می‌شود.

• ناهنجاری‌های تجمعی: زمانی که مجموعه‌ای از داده‌های شبیه به هم در نسبت با بقیه داده‌ها ناهنجار رفتار می‌کنند. برای مثال پولشویی نمونه‌ای از این دست ناهنجاری است.

دسته‌ای از روش‌ها تنها امتیاز یا احتمال ناهنجاری را به هر داده منتسب می‌کنند، در حالی که دسته‌ای دیگر، یکی از دو برچسب هنجار یا ناهنجار را.

به طور کلی الگوریتم‌های یادگیری ماشین به سه دسته تقسیم‌بندی می‌شوند:

۱. دسته اول الگوریتم‌های با ناظر هستند که در آنها از داده‌های برچسب‌خورده استفاده می‌شود. به عبارت بهتر، برای آموزش این دسته از الگوریتم‌ها که به الگوریتم‌های کلاس‌بندی نیز معروفند، از هر دو نوع داده هنجار و ناهنجار (داده‌ای که نشانگر تقلب

1.Javelin strategy & research

در سیستم مالی باشد) استفاده می‌شود. هرچند این الگوریتم‌ها کارایی بالایی دارند اما به طور ذاتی دو مشکل عمده در رابطه با این الگوریتم‌ها وجود دارد؛ اول اینکه در بسیاری از سیستم‌های مالی موجود، برچسب‌هایی تحت عنوان هنجار یا ناهنجار نگه‌داری نمی‌شوند. دوم اینکه حتی اگر این برچسب‌ها در طول زمان جمع‌آوری نیز شوند، تعداد داده‌های ناهنجار به مراتب کمتر از داده‌های هنجار است.[۳] همه الگوریتم‌های با ناظر برای این نوع داده‌ها مناسب نیست. برای مثال درختان تصمیم[۲] مانند C۴٫۵ نمی‌توانند با داده‌های نامتعادل کار کنند[۴] اما الگوریتم‌هایی نظیر ماشین بردار پشتیبان[۳] (SVM) یا شبکه عصبی مصنوعی گزینه‌های بهتری هستند.[۵] علاوه بر روش‌های مذکور، روش‌های مبتنی بر قوانین[۴] نیز در مواردی که الگوهای شناخته‌شده وجود داشته باشند روش‌های مفیدی هستند.

۲. دسته دوم الگوریتم‌های نیمه نظارتی هستند. در این نوع الگوریتم‌ها تنها لازم است که داده‌های هنجار، بدون داده‌های ناهنجار در نظر گرفته شوند. ایده این دسته از الگوریتم‌ها به‌دست‌آوردن الگوهای موجود در داده‌های هنجار است. از این طریق می‌توان داده‌هایی را که از این الگو تبعیت نمی‌کنند، داده‌های ناهنجار در نظر گرفت. به این الگوریتم‌ها کلاس‌بندی تک کلاسه نیز می‌گویند. معروف‌ترین الگوریتم‌ها در این دسته ماشین بردار پشتیبان تک کلاسه و رمزنگار خودکار[۵] است.[۶]

۳. دسته سوم الگوریتم‌های یادگیری ماشین، الگوریتم‌های بدون ناظر است که بدون هیچ گونه برچسبی سعی در شناسایی ناهنجاری‌ها دارد. با توجه به چالش‌های ذکرشده، این دسته از الگوریتم‌ها پراستفاده‌ترین روش در تشخیص ناهنجاری‌هاست که خود به دو دسته کلی تقسیم می‌شوند:

۱- روش‌های مبتنی بر نزدیک‌ترین همسایه: در این روش‌ها که شامل الگوریتم‌هایی نظیر Local Outlier Factor، Connectivity-Based Outlier Factor ، Influenced Outliers، Local Correlation Integral، Local Outlier Probability هستند، داده ناهنجار بر اساس محاسبه فاصله، چگالی کلی و محلی شناسایی می‌شوند.[۷]

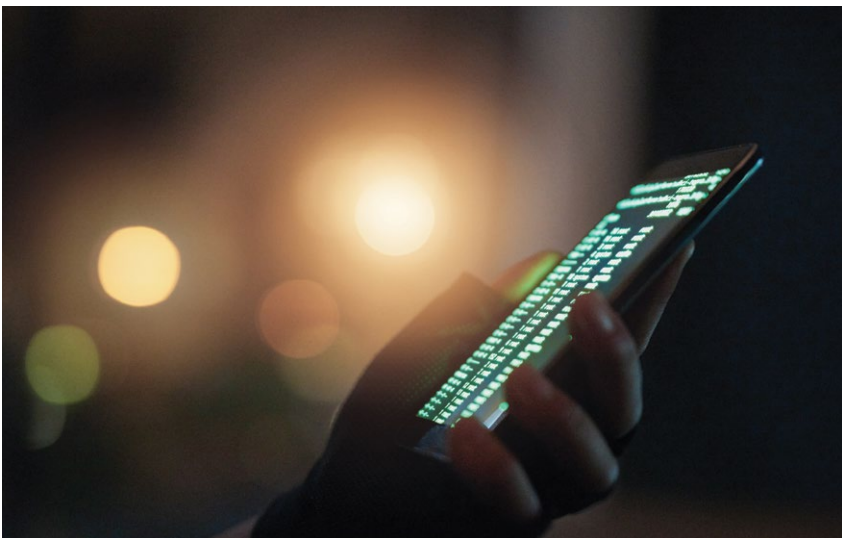
۲- روش‌های خوشه‌بندی: در روش‌های نزدیک‌ترین همسایه ابتدا بر اساس فاصله، مجموعه‌ها شناسایی و با استفاده از چگالی هر مجموعه داده‌های ناهنجار شناسایی می‌شوند. اما در روش‌های خوشه‌بندی ابتدا خوشه‌ها شناسایی و سپس درون هر خوشه، چگالی محلی محاسبه می‌شود. در مرحله بعد، با استفاده از چگالی محلی، داده‌های ناهنجار شناسایی می‌شوند. از جمله این روش‌ها می‌توان به الگوریتم‌های Histogram-based Outlier Score و Cluster-Based Local Outlier Factor اشاره کرد.

2.Decision trees
3. Support vector Machine
4.Rule based algorithms
5.Autoencoder

۳- علاوه بر موارد مذکور، روش تجزیه‌وتحلیل گروه همتا[6] نیز در دسته الگوریتم‌های بدون ناظر قرار می‌گیرد. در این روش، نیاز نیست رفتار معمول هر یک از افراد به صورت جداگانه شناسایی شود، بلکه رفتار جمعی گروهی از همتایان که در گذشته شبیه به یکدیگر رفتار کرده‌اند به عنوان مرجع در نظر گرفته می‌شود. انحراف شدید از رفتار جمعی گروه همتایان می‌تواند نشان‌دهنده ناهنجاری، یا به عبارت دیگر بروز تقلب باشد.

روش های مبتنی برگراف: این روش‌ها نیز بر اساس وجود یا عدم وجود برچسب برای داده‌ها، در سه دسته الگوریتم‌های بدون ناظر، نیمه نظارتی و با ناظر جای می‌گیرند. با این حال به دلیل اهمیت این دسته از روش‌ها به بررسی آنها به صورت جداگانه می‌پردازیم. این دسته از الگوریتم‌ها که از شبکه‌های ارتباطی برای شناسایی رفتارهای ناهنجار استفاده می‌کنند، پرکاربردترین روش‌ها برای تشخیص ناهنجاری هستند. روش‌های مبتنی بر گراف روی گراف‌های ثابت یا پویا می‌توانند راس، یال، زیرگراف یا واقعه ناهنجاری را شناسایی کنند.

منظور از راس ناهنجار، راس‌هایی هستند که در مقایسه با بقیه راس‌ها، دارای ویژگی ناهنجاری هستنند. معمولا به هر راس، بر اساس ویژگی‌های آن، امتیازی برابر با میزان ناهنجاری آن راس داده می‌شود. برای مثال بر اساس نرخ یال‌های ورودی به خروجی. مانند راس‌ها، یال‌های ناهنجار نیز با استفاده از ویژگی‌های غیرمعمول یال‌ها، برای مثال امتیازی بالاتر از یک آستانه، یافت می‌شوند. به بیانی دیگر، بعد از امتیازدهی به یال‌ها با



6.Peer group analysis

استفاده از پارامتر های مختلف همچون فاصله یا هزینه و غیره، یال‌هایی که امتیازی بالاتر از حد معمول به دست آورند می توانند به عنوان یال‌های ناهنجار شناسایی شوند. بعد از شناسایی یال‌های ناهنجار می‌توان راس‌های محتمل برای ناهنجاری را نیز یافت. برای یافتن زیرگراف‌های ناهنجار، ابتدا زیرگراف‌ها با الگوریتم‌های تشخیص انجمن[۷]، شناسایی شده، سپس به هر یک امتیازی برای میزان ناهنجاری اختصاص داده می‌شود. دسته آخر این مجموعه که تنها در گراف‌های پویا قابل اجراست، تشخیص بازه زمانی است که در آن تغییر چشم‌گیری در شبکه ایجاد شده است.

بسیاری از روش‌های مبتنی بر گراف، همان روش‌های یادگیری ماشین هستند که روی گراف پیاده‌سازی شده‌اند. بر اساس دردسترس‌بودن برچسب داده‌ها، ماهیت شبکه و نوع ناهنجاری، روش‌های مختلفی به کار برده می‌شود. برای مثال می‌توان از روش‌های ساختاری که بر اساس ویژگی‌های توپولوژی، شبکه راس‌ها و یال‌های ناهنجار را شناسایی می‌کنند یا روش‌های آماری که بر اساس تئوری احتمالات، توزیع احتمالات و... مدلی برای رفتار به هنجار می‌سازد و سپس هر انحرافی از این رفتار را به عنوان رفتار ناهنجار شناسایی می‌کنند، نام برد[۸].

منابع:

.[1]Bolton RJ, Hand DJ. Unsupervised profiling methods for fraud detection. Credit scoring and credit control VII. 2001 Sep 5:235-55.

.[2] https://www.javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study

.[3] Anandakrishnan A, Kumar S, Statnikov A, Faruquie T, Xu D. Anomaly detection in finance: editors' introduction. InKDD 2017 Workshop on Anomaly Detection in Finance 2018 Jan 7 (pp. 1-7). PMLR.

.[4] Ross Quinlan J. C4. 5: programs for machine learning. Mach. Learn. 1993 Jan;16(3):235-40.

.[5] Schölkopf B, Smola AJ, Bach F. Learning with kernels: support vector machines, regularization, optimization, and beyond. MIT press; 2002

.[6] Hawkins S, He H, Williams G, Baxter R. Outlier detection using replicator neural networks. InInternational Conference on Data Warehousing and Knowledge Discovery 2002 Sep 4 (pp. 170-180). Springer, Berlin, Heidelberg.

.[7] Goldstein M, Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS one. 2016 Apr 19;11(4):e0152173.

.[8] Pourhabibi T, Ong KL, Kam BH, Boo YL. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems. 2020 Jun 1;133:113303.

7.Community detection

مروری بر راهکارهای اصلی مقابله با تقلب در حوزه بانکی و بیمه‌ای

مرکز مطالعات و تحقیقات داتین

امروزه به دلیل گسترش زیرساخت‌های اینترنت و استفاده از موبایل، ذخیره‌سازی اطلاعات مربوط به فعالیت‌های مشتریان توسط شرکت‌های ارائه‌دهنده خدمات مالی با سهولت بیشتری انجام می‌پذیرد. از اهداف اصلی گردآوری و پردازش اطلاعات می‌توان به درک بهتر الگوهای رفتاری مشتریان و ارائه‌دهندگان خدمات مالی اشاره کرد که نقش مهمی در شناسایی تقلب‌های مالی صورت‌گرفته توسط آنان دارد. شناسایی و جلوگیری از تقلب می‌تواند دارایی‌های شرکت‌ها را حفظ کرده و سطح اعتماد به خدمات مالی ارائه‌شده را افزایش دهد.

در پژوهش حاضر ابتدا به معرفی مهم‌ترین موارد تقلب در حوزه مالی به همراه درصد افزایش آنها در سال ۲۰۲۱ پرداخته شده است؛ سپس دو الگوی اصلی که تقلب‌های مالی بر پایه آن صورت می‌پذیرد مورد تحلیل قرار گرفته است. در گام بعدی اثرات منطقه‌ای و راهکارهای کشورهای منتخب برای مقابله با تقلب‌های مالی بررسی شده است و در پایان جمع‌بندی و نتیجه‌گیری نهایی صورت گرفته است.

مروری بر آمار تقلب در حوزه مالی

تقلب‌های مالی امروزه در سطح گسترده‌ای صورت می‌پذیرد. هکرها برای دست‌یابی به منابع مالی افراد و شرکت‌ها، مشتریان با هدف استفاده چندین باره از خدمات و فروشندگان با هدف اخذ پول‌های بیشتر از مشتریان اقدام به تقلب مالی می‌کنند. مهم‌ترین عنوان‌هایی که تقلب‌های مالی در آن صورت می‌گیرد در ۱۰ حوزه اصلی در جدول یک طبقه‌بندی شده است.

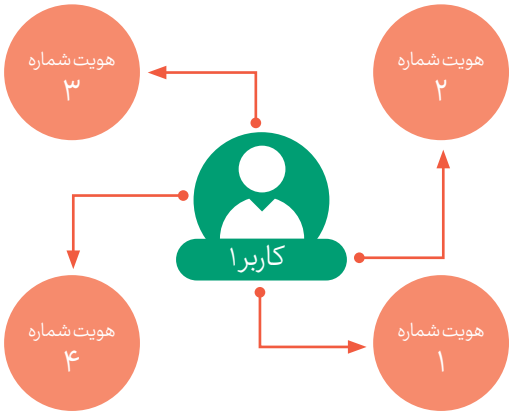
جدول۱-۱۰ حوزه اصلی تقلب و درصد افزایش آنها در گزارش بررسی تقلب و جرم اقتصادی جهانی ۲۰۲۲

رتبه	عنوان	درصد	رتبه	عنوان	درصد
۱	هکرها	۳۱	۶	رقیبان	۱۴
۲	مشتریان	۲۹	۷	سرمایه‌گذاری‌های مشترک و شرکای تجاری	۱۲
۳	جرایم سازمان یافته	۲۸	۸	ارائه‌دهندگان خدمات اشتراکی	۱۲
۴	عرضه کنندگان و فروشندگان	۲۰	۹	مشاوران	۱۰
۵	کارگزاران و واسطه‌ها	۱۵	۱۰	دولت‌های خارجی	۹

Source: Global Economic Crime and Fraud Survey 2022

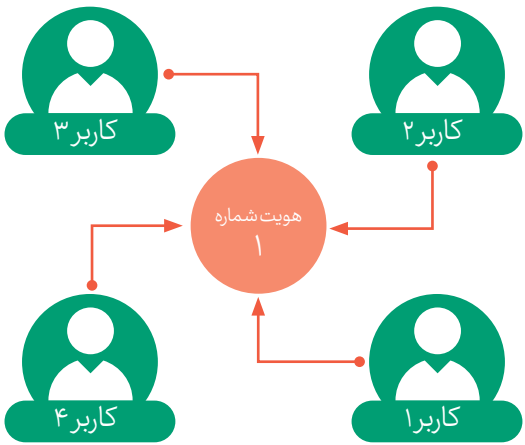
همان گونه که جدول یک نمایش می‌دهد در سال ۲۰۲۲، بیشترین رشد به ترتیب در بخش‌های حمله‌های هکری با ۳۱ درصد، مشتریان با ۲۹ درصد و جرایم سازمان‌یافته با ۲۸ درصد رخ داده است که دلالت بر تمرکز تقلب‌ها در حوزه‌های یادشده در سطح بین‌المللی دارد. همچنین تقلب در مواردی همچون سرمایه‌گذاری‌های مشترک و شرکای تجاری با ۱۲ درصد، ارائه‌دهندگان خدمات اشتراکی با ۱۲ درصد، مشاوران با ۱۰ درصد و دولت‌های خارجی با ۱۰ درصد نسبت به سایر موارد، اهمیت کمتری در این زمینه دارا هستند.

تقلب‌های حوزه مالی را می‌توان به دو دسته عمده تقسیم‌بندی کرد؛ دسته نخست تقلب‌های آگاهانه هستند. در تقلب‌های آگاهانه فرد یا گروه با قصد و نیت قبلی اقدام به برنامه‌ریزی برای انجام آن می‌کند. در دسته دوم هویت فرد توسط فرد یا گروهی مورد سوءاستفاده قرار می‌گیرد و وی هیچ اطلاعی از این موضوع ندارد. با توجه به دسته‌بندی یادشده دو الگوی عمده بیش از سایر الگوهای تقلب مورد استفاده قرار می‌گیرند. این موضوع در شکل یک و شکل دو نمایش داده شده‌اند. همان گونه که مشاهده می‌شود در الگوی نخست، کاربر از چند هویت برای دست‌یابی به اهداف خود استفاده می‌کند. به عنوان مثال فرد برای دریافت وام یا خدمتی خاص به کمک چند هویت، سامانه‌های تشخیص تقلب را فریب می‌دهد.



شکل۱- الگوی یک کاربر به همراه چند هویت جعلی

در الگوی دوم چند کاربر از یک هویت واحد برای تقلب در سامانه استفاده می‌کنند. برای مثال چند نفر از یک دفترچه خدمات درمانی استفاده می‌کنند.



شکل۲- الگوی استفاده همزمان چند کاربر از یک هویت واحد

راهکارهای مقابله با تقلب‌های بانکی و بیمه‌ای

با توجه به الگوهای اشاره‌شده امروزه روش‌های گوناگونی برای مقابله با تقلب در حوزه مالی مورد استفاده قرار می‌گیرد. کیفیت طراحی سامانه‌ها و روش‌های مقابله با تقلب در جهان، به دلایلی همچون تفاوت در سطح فناوری کشورها و دانش سرمایه انسانی، دارای اثرات منطقه‌ای است.

در جدول دو راهکارهای عمده مقابله با تقلب در سطح بین‌الملل بر اساس اولویت در کشورهای منتخب نمایش داده شده است. همان گونه که مشاهده می‌شود در بیشتر مناطق به ویژه کشورهای اروپایی، هند، برزیل و استرالیا افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال و سرمایه گذاری در نرم‌افزار تشخیص تقلب و روش‌ها از راهکارهای اصلی برای مقابله با تقلب‌های بانکی و بیمه‌ای در نظر گرفته شده است.
در آمریکا و سنگاپور تمرکز سرمایه‌گذاری‌ها در نرم‌افزارهای دیجیتال تصمیم‌گیری مورد توجه بوده است. همچنین افزایش کارکنان مرکز تماس و پشتیبانی در آمریکا و افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال در سنگاپور برای مقابله با تقلب به صورت ویژه مورد استفاده قرار گرفته است.
راهکارهایی که برای مقابله با تقلب‌های بانکی در اسپانیا و انگلستان مورد استفاده قرار گرفته، افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال است و در ژاپن سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته و هوش مصنوعی اولویت اصلی قرار گرفته است.

جدول۲- راهکارهای مقابله با تقلب بر اساس اولویت در کشورهای منتخب

هند	آلمان	فرانسه	برزیل	استرالیا
افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته و هوش مصنوعی
سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها
آمریکا	**انگلستان**	**اسپانیا**	**سنگاپور**	**ژاپن**
سرمایه‌گذاری در نرم‌افزارهای دیجیتال تصمیم‌گیری	سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته و هوش مصنوعی
افزایش کارکنان مرکز تماس و پشتیبانی	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته و هوش مصنوعی	سرمایه‌گذاری در نرم‌افزارهای دیجیتال تصمیم‌گیری	افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال

Source: Global Identity and Fraud Report 2022

همچنین با هدف بررسی دقیق‌تر در جدول سه راهکارهای مقابله با تقلب به ترتیب اولویت برای کسب‌وکارهای جهانی در سال ۲۰۲۲ در هفت دسته اصلی متمرکز شده است. نتایج جدول بر اساس متوسط جهانی از بیشترین به کمترین درصد افزایش، مرتب شده است. مشاهده می‌شود سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته با ۵۲ درصد، هوش مصنوعی و سرمایه‌گذاری در نرم‌افزار تشخیص تقلب با ۴۷ درصد، بیشترین تمرکز را به خود اختصاص داده‌اند. بنابراین می‌توان نتیجه گرفت تقویت بخش تحلیل و هوش مصنوعی اولویت اصلی کشورها در مقابله با تقلب در حوزه مالی است. از جمله دلایل این موضوع می‌توان به دقت بالا، حجم بالای بررسی و امکان رصد شبانه‌روزی در این روش‌ها اشاره کرد.

در اولویت‌های بعدی، افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال با ۳۳ درصد و سرمایه‌گذاری در نرم‌افزارهای دیجیتال تصمیم‌گیری[1] با ۳۰ درصد افزایش قرار گرفته‌اند که دلالت بر اهمیت نقش سرمایه انسانی در تشخیص و واکنش به تقلب را داشته و اهمیت تصمیم‌گیری در این حوزه را نمایش می‌دهد.

در انتهای جدول نیز افزایش کارکنان مرکز تماس و پشتیبانی با ۲۷ درصد، افزایش پرسنل در شعبه با ۲۳ درصد و حل میراث به‌جای‌مانده از مسائل تکنولوژی با ۲۳ درصد قرار گرفته که دلالت بر نقش موثر سرمایه انسانی در تشخیص تقلب و تشدید نظارت‌ها در این حوزه دارد.

جدول۳- راهکارهای مقابله با تقلب بر اساس اولویت در کشورهای منتخب بر حسب درصد

	آمریکا	انگلستان	اسپانیا	سنگاپور	ژاپن	هند	آلمان	فرانسه	برزیل	استرالیا	جهان
سرمایه‌گذاری در تجزیه‌وتحلیل پیشرفته و هوش مصنوعی	٪۵۴	٪۴۴	٪۴۶	٪۵۴	٪۵۸	٪۶۰	٪۴۱	٪۵۲	٪۶۰	٪۵۳	٪۵۲
سرمایه‌گذاری در نرم‌افزار تشخیص تقلب و روش‌ها	٪۴۰	٪۴۳	٪۳۷	٪۴۴	٪۳۶	٪۵۳	٪۵۲	٪۵۰	٪۶۶	٪۵۲	٪۴۷
افزایش کارکنان داخلی و پشتیبانی برای عملیات دیجیتال	٪۳۶	٪۳۰	٪۲۹	٪۳۶	٪۳۶	٪۴۹	٪۲۳	٪۳۱	٪۳۷	٪۳۰	٪۳۳
سرمایه‌گذاری در نرم‌افزارهای دیجیتال تصمیم‌گیری	٪۳۹	٪۲۳	٪۲۶	٪۳۷	٪۲۹	٪۳۰	٪۲۲	٪۲۶	٪۳۴	٪۲۶	٪۳۰
افزایش کارکنان مرکز تماس و پشتیبانی	٪۳۹	٪۳۰	٪۲۶	٪۲۶	٪۱۷	٪۴۲	٪۲۰	٪۲۳	٪۲۶	٪۲۲	٪۲۷
افزایش پرسنل در شعبه	٪۳۱	٪۲۳	٪۲۳	٪۲۶	٪۲۰	٪۲۴	٪۲۱	٪۲۰	٪۱۹	٪۲۱	٪۲۳
حل میراث به‌جای‌مانده از مسائل تکنولوژی	٪۲۱	٪۲۲	٪۲۷	٪۲۳	٪۲۶	٪۳۰	٪۱۹	٪۲۱	٪۲۳	٪۲۲	٪۲۳

Source: Global Identity and Fraud Report 2022

1.Digital Decisioning Software

جمع‌بندی و نتیجه‌گیری

با گسترش تقلب در حوزه مالی، راهکارهای مقابله با آن نیز در سطح بین‌المللی گسترش یافته است. بررسی دقیق‌تر این موضوع نشان‌دهنده تفاوت‌های منطقه‌ای در راهکارهای مقابله با تقلب‌های مالی موجود است و کشورها با سرمایه‌گذاری در بخش‌های گوناگون و بر پایه نقاط قوت و ضعف خود به تهدیدها پاسخ می‌دهند. سرمایه‌گذاری‌ها به صورت عمده با دو رویکرد نرم‌افزاری و سرمایه انسانی صورت پذیرفته که تا حد ممکن این مسئولیت به هوش مصنوعی و نرم‌افزارهای تحلیل واگذار شده است. در اولویت‌های بعدی نقش سرمایه انسانی متخصص در بخش پشتیبانی جلب توجه می‌کند زیرا همچنان نیاز به حضور انسان برای تصمیم‌گیری و شناسایی تقلب‌ها احساس می‌شود.

یافته‌های پژوهش به صورت زیر جمع‌بندی می‌شود:

• با توجه به افزایش درصد تقلب‌های مالی در کشورهای مختلف، مقابله با تقلب یک دغدغه بین‌المللی است.

• بسیاری از تقلب‌ها از الگوهای مشابهی پیروی می‌کنند؛ از این رو در بسیاری از کشورها برای مقابله با این دسته از تقلب‌ها، از راهکارهای مشابه استفاده می‌شود.

• در عین حال بخشی از تقلب‌ها به دلیل وجود اثرات منطقه‌ای، تفاوت فناوری و نوع تهدیدها، یک مسئله بومی هستند؛ بدین معنی که نسخه واحدی برای مقابله با آنها در کشورها و شرکت‌ها وجود ندارد و به صورت مطالعه موردی بررسی می‌شوند.

همچنین موارد زیر پیشنهاد می‌شود:

• سرمایه‌گذاری روی بخش توسعه نرم‌افزارها به ویژه نرم‌افزارهای تحلیلی و هوش مصنوعی در اولویت قرار گیرد زیرا گستره تحت پوشش و حجم شناسایی تقلب توسط چنین نرم‌افزارهایی بسیار زیاد است.

• از منظر تحلیل زمان تقلب، از آنجا که سامانه‌های شناسایی تقلب به صورت برخط و ۲۴ ساعته به بررسی تقلب‌های مالی می‌پردازند، از این رو برای مقابله با تهدید به عنوان یکی از اولویت‌های سرمایه‌گذاری پیشنهاد می‌شوند.

• سرمایه انسانی متخصص در دپارتمان‌های مشخص با وظایف از پیش تعریف‌شده برای مقابله با آن دست از تهدیدهایی که امکان شناسایی آن توسط نرم‌افزار وجود ندارد آموزش ببینند.

• آمارهای کلیدی ایران همچون جمعیت تقریبی ۸۴ میلیون نفری و ضریب نفوذ ۱۶۶ درصدی تلفن همراه، مؤید این است که ارائه بهینه خدمات و نظارت بر تقلب‌های احتمالی نیازمند استفاده از هوش مصنوعی و سرمایه‌گذاری گسترده در بخش توسعه نرم‌افزاری است.

• از سوی دیگر با توجه به ظرفیت‌های بالای سرمایه انسانی متخصص و تحصیل‌کرده در

ایران، پیشنهاد می‌شود در مسائل نظارتی و تحلیلی که امکان استفاده از نرم‌افزار وجود ندارد، از راهکار افزایش سرمایه انسانی آموزش‌دیده استفاده شود.

• امروزه طیف گسترده‌ای از صنایع در ایران مشغول به فعالیت هستند. به دلیل تفاوت در سطح فناوری آنها، پیشنهاد می‌شود برای هر یک به صورت بومی و متناسب با نیاز هر سازمان، روش‌های مقابله با تقلب طراحی و پیاده‌سازی شود.

منابع

Haller, Eric. (July 23, 2022), Experian Global Identity Fraud Report. (2021). https://www.experian.com/decision-analytics/global-fraud-report

Piper, Charles E. (2016). Healthcare fraud investigation guidebook, CRC Press

River, Kristin. (July 20, 2022), PwC's Global Economic Crime and Fraud Survey. (2022). https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Westphal, C. (2008). Data Mining for Intelligence, Fraud & Criminal Detection: Advanced .Analytics & Information Sharing Technologies. CRC Press

گفت‌وگوی «فناوری‌های مالی» با علیرضا بادامچی، مدیر پروژه کشف تخلف و تقلب شاپرک

سامانه کشف تخلف و تقلب به حفظ وجهه اجتماعی بانک هم کمک می‌کند

شرکت شاپرک (شبکه الکترونیکی پرداخت کارت) در دی‌ماه ۱۳۹۰ به عنوان بازوی بانک مرکزی تشکیل شد و اکنون پس از یک دهه فعالیت، نقشی محوری در محقق‌ساختن فرامین و مقررات ملی و حاکمیتی در موضوع پرداخت الکترونیکی دارد.

نقش این شرکت به عنوان بازوی فنی و تخصصی رگولاتور در موضوع شناسایی تراکنش‌های مشکوک و کشف تخلف و تقلب بسیار پررنگ است. در این مطلب با علیرضا بادامچی، مدیر پروژه کشف تخلف و تقلب شاپرک، پیرامون اهمیت وجود چنین سامانه‌ای در نظام پرداخت الکترونیکی کشور گفت‌وگو کرده‌ایم.

■ **طبق چه استاندارد یا معیاری، یک تراکنش مشکوک تلقی می‌شود؟**

تراکنش مشکوک به سه دسته تقلب، تخلف و پولشویی تقسیم می‌شود. تخلف وقتی است که یک قانون نقض می‌شود. مثال آن این است که برای دریافت وام باید وثیقه داده شود اما این اتفاق نمی‌افتد یا میزان وثیقه از اندازه اعلام‌شده کمتر است که هر دوی این‌ها تخلف از قانون است. تقلب زمانی رخ می‌دهد که یک شخص، گروه یا کل جامعه از تراکنشی که در حال انجام است متضرر شوند. مثال آن انجام قمار با یک تراکنش است یا وقتی که پول بدون اینکه شخص بداند از یک حساب به حساب دیگری منتقل شود. مورد دیگر پولشویی است. یعنی یک عمل متقلبانه انجام شده و می‌خواهند پول را در فرایند مالی بانک و شبکه پرداخت بشورند. در حقیقت هدف، پاکسازی پول یا فرار مالیاتی است. عموما در این کار یا مبدا پول مشخص نیست یا این کار را انجام می‌دهند که مبدا را از بین ببرند.

■ **این تعاریف به طور عمومی برای تمام سامانه‌های کشف تقلب و تخلف در نظام بانکی ایران صادق است؟**

بله؛ تقلب‌های ما دو بخش داخلی و خارجی دارد. تقلب داخلی که توسط کارمندان صف و ستاد انجام می‌شود. این تقلب‌ها به‌شدت به بانک ضرر مالی می‌زند و این نرم‌افزارها به بانک کمک می‌کند تا متضرر نشوند. در این میان الزام بانک مرکزی بیشتر تقلب‌های خارجی است که از سوی مشتریان بانک است؛ یعنی بیشتر تقلب‌های کارت.

■ **بیشتر کدام موارد در ایران رخ می‌دهد؟**

بحث بیشتر روی اجبارهایی است که بانک مرکزی گذاشته است. بانک مرکزی بیش از همه روی پولشویی حساس است تا بتواند رد آنها را پیدا کند. در حال حاضر بانک‌ها و شبکه پرداخت نرم‌افزار پولشویی را بیش از نرم‌افزارهای کشف تقلب و تخلف در اختیار دارند که این هم به دلیل تاکیدات بانک مرکزی است.

■ **سامانه کشف تقلب از پولشویی جداست؟**

می‌توانند همه آنها یکی باشند، ولی در حال حاضر در صنعت بانکی، به عنوان دو محصول مختلف شناخته می‌شوند. کشف تقلب و تخلف، در لحظه عمل مجرمانه اتفاق می‌افتد، اما در سیستم‌های مبارزه با پولشویی عمل مجرمانه رخ داده و می‌خواهند منبع آن را پاک کنند.

■ **به نظر می‌رسد در حوزه مبارزه پولشویی قوانین مشخص داریم و تولیدکننده نمی‌تواند خارج از چارچوب عمل کند. اما در حوزه کشف تقلب و تخلف، به‌دلیل وجود پارامترهای گسترده، تولیدکننده نرم‌افزار می‌تواند ویژگی‌هایی را به محصول خود بیفزاید.**

بله همین‌طور است. در بحث مبارزه با پولشویی، بانک مرکزی خیلی قبل‌تر، قواعدی را برای بانک‌ها ارسال کرده و آنها در این حوزه، سیستم‌های خود را دارند. البته در نرم‌افزار پولشویی خودشان سراغ ابتکارها می‌روند. مثلا خودشان سراغ محاسبه ریسک می‌روند که ریسک پولشویی هر تراکنش چقدر است که می‌شود پولشویی ریسک‌محور. در حوزه کشف تقلب و تخلف حدود دو سال است که بانک مرکزی ارسال بخش‌نامه و ملزم‌کردن بانک‌ها به فعالیت در این زمینه را آغاز کرده است. بانک مرکزی و وزارت اقتصاد هم بانک‌ها را ملزم به داشتن این سامانه کرده‌اند.

■ **به نظر می‌رسد بانک‌ها خیلی سراغ این موضوع نمی‌روند چراکه بیشتر الزامات، مربوط به تقلب و تخلف خارجی است. به نظر می‌رسد بانک در این حوزه خیلی ضرر نمی‌کند. اینجا چون رگولاتوری روی کشف تقلب خارجی تاکید دارد بانک هم انگیزه‌ای برای رفتن به این سامانه‌ها ندارد.**

یک بحث ضرر مالی است و بحث دیگر آسیب به وجهه اجتماعی بانک به خاطر تخلفات و تقلب‌های داخلی. این تقلب‌ها زمانی مشخص می‌شود که حجم بسیار زیادی از پول از بانک خارج می‌شود. برای همین، سامانه‌های کشف تخلف و تقلب می‌توانند هم جلوی ضرر مالی بانک را بگیرند و هم به حفظ وجهه اجتماعی آنها کمک کنند.

■ **پس چرا الزام بانک مرکزی بیشتر روی کارت است؟**

چون بیشتر تراکنش‌های شبکه بانکی روی کارت است. ما ۱۵۰ میلیون تراکنش روزانه داریم که حدود ۱۲۰ میلیون آن تراکنش کارتی است. بنابراین ابتدا باید سراغ کارت برویم.

■ **از میان ۱۵۰ میلیون تراکنش، چه میزان تراکنش، تقلب و تخلف و پولشویی است؟**

برای این میزان نمی‌توان عدد دقیق ارائه داد. اما اگر حتی یک درصد را تراکنش مشکوک لحاظ کنیم، روزانه یک میلیون و نیم تراکنش مشکوک داریم. البته همه این تراکنش‌ها ضرورتا تخلف یا تقلب نیستند، بلکه تراکنش‌هایی هستند که باید بررسی شوند.

■ **این بررسی‌ها به صورت دستی است یا آنلاین؟**

به دو روش انجام می‌شود. بخش اول توسط یک فرد مجرب انجام می‌شود و بخش دیگر توسط هوش مصنوعی. این مشکوک‌بودن جنبه‌های مختلف دارد. مثلا وقتی است که مانده یک حساب، یک میلیون تومان بوده ولی بعد از چند سال دو میلیارد تومان به حساب آن واریز می‌شود. در این شرایط تخلفی انجام نشده اما تراکنش، مشکوک به نظر می‌رسد و باید بررسی شود. مثلا اسناد واریز باید بررسی شود. این را شاید فرد مجرب بتواند ببیند اما هوش مصنوعی نه. ممکن است گردش زیادی در یک حساب اتفاق بیفتد. مثلا گردش حساب در یک بازه زمانی در حساب زیاد باشد و به یک باره متوقف شود. برای مثال ما تعداد زیادی تقلب و تخلف داریم که در کارت‌های کرایه‌ای انجام می‌شود.

■ **آیا یکی از دلایل آن می‌تواند این باشد که کارت تنها ابزاری است که متکی به فرد نیست و می‌تواند بدون حضور او هم استفاده شود؟**

بله. البته رمز دوم پویا این مساله را پوشش می‌دهد و تقلب‌هایی را که در این زمینه انجام می‌شود کمتر کرده است.

■ **آیا این امکان وجود دارد که سامانه‌های کشف تقلب و تخلف جایگزین افراد مجرب شوند؟**

این موضوع باید گام‌به‌گام جلو برود. ما نمی‌توانیم بگوییم که یک سامانه کشف تقلب و تخلف می‌گذاریم و این سامانه کاملا به‌درستی تقلب و تخلف‌ها را تشخیص می‌دهد. اینکه ما بگوییم یک کارت با بالای ۹۰ درصد تراکنش مشکوک، بسته شود کاری است که ماشین می‌تواند انجام دهد. جایی هم هست که یک فرد مجرب باید برود، اسناد را ببیند و اگر به نظر او مساله‌ای وجود نداشت آن را به سیستم ارائه می‌دهد و سیستم دفعه بعد آن را تقلب نشان نمی‌دهد. بحث یادگیری ماشین است و روز اول شاید پرفورمنس سیستم ۶۰ درصد باشد و سه ماه بعد بشود ۷۰ درصد و مداوم به صورت تصاعدی بالا برود.

■ **در ماجرای پولشویی، قواعد مشخص وجود دارد. آیا در موضوع کشف تقلب و تخلف ایجاد یک سامانه یکپارچه منطقی است یا نه؟**

می‌تواند منطقی باشد، اما بهتر این است که ماژول‌بیس باشد. ما به ازای هر ماژولی می‌توانیم این را بنویسیم. برای مثال، ماژول کشف تقلب چک، ساتنا، پایا و... را بگذاریم. یک استانداردی داشته باشیم با یک ورودی و یک خروجی. این ماژول‌ها هم با هم ارتباط داشته باشند.

■ **در این زمینه چه همکاری مشترکی بین رگولاتور و بانک‌ها وجود دارد؟**

رگولاتور در حال بررسی و پیگیری نتیجه از بانک‌هاست. بخش‌نامه‌هایی که داده بیشتر سمت سناریوهای تقلب بوده است، آن هم بیشتر کارتی و سنجش با پروفایل مشتری. هنوز هم با اینکه رگولاتوری هیچ بانکی را ملزم نکرده که کشف تقلب آنلاین داشته باشد، بسیاری از بانک‌ها سامانه کشف تقلب آنلاین دارند.

■ **خیلی مهم است که رگولاتور و بانک روی مزایای اقتصادی و اجتماعی مبارزه با تخلف تمرکزکنند؟**

بله اما سامانه‌های کشف تقلب هم باید بهینه طراحی شوند، خطای سیستم خیلی کم باشد و باعث نشود فعالینی که تقلب یا تخلف ندارند، متضرر شوند.

به نظر شما مجموعه فعالیت‌هایی که تا امروز انجام شده باعث کاهش تقلب شده است؟

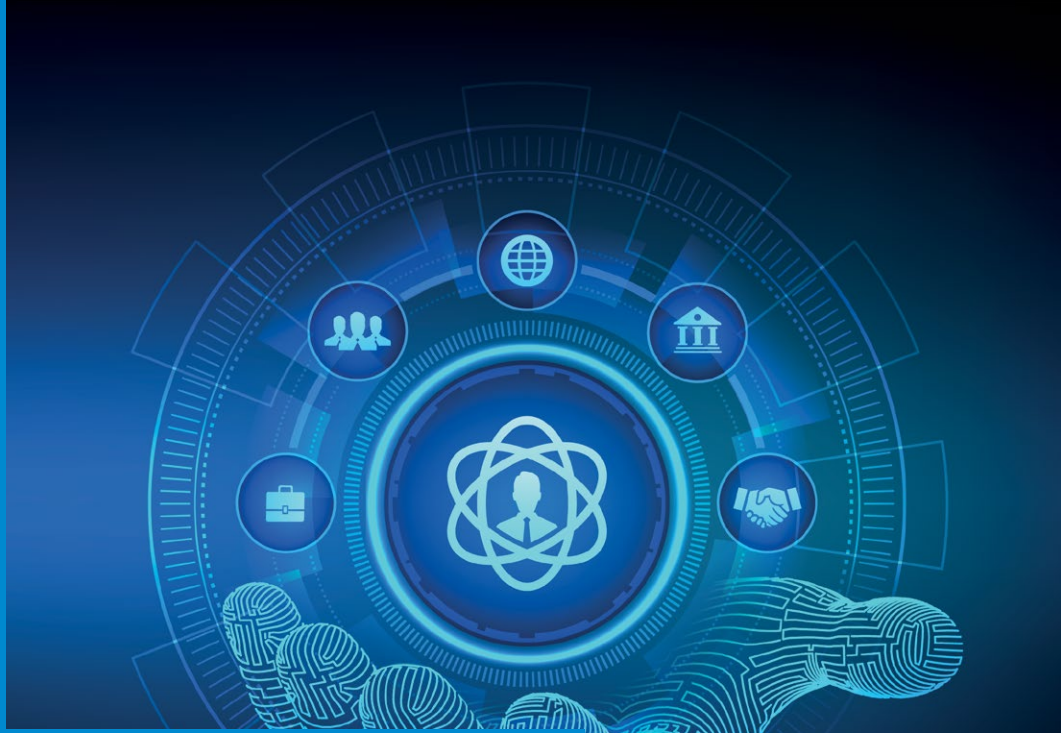
بله قطعا؛ اما یک نکته وجود دارد. اینکه متقلب همیشه یک قدم از سامانه کشف تقلب و تخلف جلوتر است. وقتی جلوی تقلب را بگیرید سراغ یک تقلب دیگر می‌روند. سیستم باید طوری طراحی شود که جلوی قدم‌های بعدی متقلب را بتوانیم بگیریم.

رگولاتوری از بانک‌ها در این زمینه چه انتظاری دارد؟

قاعدتا انتظارات، همان بخش‌نامه‌های بانک مرکزی است که خروجی‌ها را هم کنترل می‌کند. اما هنوز الزامی برای استفاده آنلاین از این سامانه وجود ندارد. سیستم کشف تقلب آنلاین معمولا در حوزه کارت و مشتری است، اما برای بانک این موضوع اهمیت ندارد چون خودش ذی‌نفع نیست و ضرر نمی‌کند. ضرر برای بانک این است که جلوی خیلی از تراکنش‌ها از این طریق گرفته می‌شود. از طرف دیگر خواست بانک مرکزی این است که بانک‌ها در زمینه آنلاین به بلوغ برسند و بعد سراغ آن بروند.

مسیر کشف تقلب در شاپرک به چه صورت است؟

ما یک نرم‌افزار کشف تقلب داریم که هنوز آفلاین است اما داریم به سراغ این می‌رویم که آن را به صورت آنلاین هم داشته باشیم. مضاف بر اینکه خیلی از تخلف‌ها و تقلب‌ها را بر اساس هوش مصنوعی کشف می‌کنیم. مباحث سامانه ما بیشتر کشف فرار مالیاتی است و اینکه به عنوان مثال، عدهای صنفشان را نادرست ثبت کرده‌اند و با پایانه‌ای که دارند، فعالیت‌های خارج از صنف انجام می‌دهند. همین‌طور صرافی‌هایی که مالیات نمی‌دهند یا پایانه‌هایی که خارج از کشور فعالیت می‌کنند. عمده فعالیت سامانه کشف تقلب شاپرک در این حوزه‌هاست.



۱۲ کاربرد هوش مصنوعی و یادگیری ماشین در حوزه مالی

امین میرزایی عسگرانی
برنامه‌نویس انبار داده داتین

در عصر دیجیتالی‌شدن این روزها به‌روزماندن کسب‌وکارها نسبت به پیشرفت‌های فناوری، تبدیل به یک ضرورت شده است. علت این ضرورت ابتدا پیشی‌گرفتن از سایر رقبا و در ادامه دست‌یابی به رشد مطلوب کسب‌وکارهاست.

در سال‌های اخیر، با پیشرفت نرم‌افزارها و سخت‌افزارها، سرعت رشد فناوری‌هایی مانند هوش مصنوعی و یادگیری ماشین در حوزه مالی افزایش یافته است. بخش مالی به طور خاص، شاهد افزایش شدیدتری از موارد استفاده از برنامه‌های کاربردی یادگیری ماشین بوده است. این افزایش شدید، منجر به دست‌یابی به نتایجی بهتر، هم به نفع مصرف‌کنندگان و هم به نفع کسب‌وکارها شده است.

یادگیری ماشین در حوزه مالی

تا همین اواخر، فقط صندوق‌های سرمایه‌گذاری، پوشش‌دهنده ریسک کاربران اصلی هوش مصنوعی و یادگیری ماشین در حوزه مالی بودند، اما در چند سال اخیر شاهد

گسترش کاربردهای یادگیری ماشین در حوزه‌های مختلف دیگر از جمله بانک‌ها، فین‌تک، رگولاتوری‌ها و شرکت‌های بیمه بوده‌ایم.
از موارد مختلف استفاده از هوش مصنوعی و یادگیری ماشین که تاثیر قابل توجهی بر بخش مالی دارند، می‌توان به موارد زیر اشاره کرد:
سرعت‌بخشیدن به فرایند پذیره‌نویسی، تشکیل و بهینه‌سازی پورتفولیو، اعتبارسنجی مدل‌ها، ربات‌های مشاور، تجزیه‌وتحلیل تاثیر بازار و ارائه روش‌های گزارش اعتباری جایگزین.
شرکت‌های فعال در صنعت مالی، از جمله بانک‌ها، شرکت‌های بازرگانی و فین‌تک‌ها، به‌سرعت الگوریتم‌های ماشینی را برای خودکارسازی فرایندهای زمان‌بر و پیش‌پاافتاده و ارائه تجربه‌ای به مراتب ساده‌تر و شخصی‌شده‌تر برای مشتری، به کار می‌گیرند.

یادگیری ماشین در حوزه مالی چگونه کار می‌کند؟

روش کار یادگیری ماشین این گونه است که با استخراج بینش‌های معنی‌دار از مجموعه داده‌های خام کار می‌کند و نتایج دقیقی را ارائه می‌دهد.
در نهایت این اطلاعات مفید استخراج‌شده از داده خام، برای حل مشکلات پیچیده از جنس داده که برای بخش بانکداری و مالی حیاتی است، استفاده می‌شود.
علاوه بر این در گذر زمان، الگوریتم‌های یادگیری ماشین با یادگیری از داده‌ها، فرایندها و تکنیک‌های فعلی مورد استفاده قوی‌تر شده و بینش‌های جدیدتری از داده‌ها را کشف می‌کنند.

چالش‌های پیش روی شرکت‌های مالی در حین اجرای راه حل‌های یادگیری ماشین

هوش مصنوعی در سازمان‌ها معمولا با مشکلات زیر همراه است:

۱. عدم درک مناسب در مورد KPI‌های کسب‌وکار

تمامی شرکت‌های خدمات مالی تمایل دارند از فرصت عالی یادگیری ماشین استفاده کنند، اما به دلیل انتظارات غیرواقعی و عدم شفافیت درمورد نحوه عملکرد هوش مصنوعی و یادگیری ماشین و چرایی نیاز به آن، اغلب در این جنبه شکست می‌خورند.

۲. هزینه بالای تحقیق‌وتوسعه

شرکت‌های خدمات مالی اغلب با مدیریت داده‌ها و ساختار تکه‌تکه ذخیره داده‌ها در قسمت‌های مختلف سازمان، مانند نرم‌افزار گزارش‌دهی، دیتاسنترهای منطقه‌ای، CRM

و... مشکل دارند. آماده‌سازی این داده‌ها برای پروژه‌های علم داده هم زمان‌بر و هم امری بسیار پرهزینه است.
ترکیب همه این چالش‌ها منجر به تخمین‌های غیر واقعی از بودجه پروژه می‌شود و کل بودجه پروژه را از بین می‌برد. شرکت‌های مالی باید انتظارات واقعی را برای هر پروژه خدمات یادگیری ماشینی متناسب با اهداف تجاری خاص خود تعیین کنند.

چرا از یادگیری ماشینی در امور مالی استفاده کنیم؟

شرکت‌های خدمات مالی و بانکی باید با وجود چالش‌های ذکرشده در بالا، از یادگیری ماشین استفاده کنند زیرا:

- باعث افزایش درآمد به دلیل بهره‌وری بهتر و بهبود تجربه کاربران می‌شود.
- باعث کاهش هزینه‌های عملیاتی به دلیل اتوماسیون فرایندها می‌شود.
- باعث تقویت امنیت و انطباق‌پذیری بهتر می‌شود.

موارد استفاده از یادگیری ماشین در حوزه مالی

در ادامه ۱۲ مورد از کاربردهای هوش مصنوعی و یادگیری ماشین مورد بررسی قرار می‌گیرد:

۱. نظارت مالی

الگوریتم‌های یادگیری ماشین به طور قابل توجهی می‌توانند برای افزایش امنیت شبکه مورد استفاده قرار بگیرند. دانشمندان داده همواره در حال کار روی سیستم‌های یادگیرنده هستند. مانند الگوریتم‌هایی که تکنیک‌های پولشویی جدید را یاد می‌گیرند. با یادگیری این تکنیک‌ها که منجر به نظارت مالی دقیق می‌شود می‌توان از این تخلفات جلوگیری کرد. در آینده احتمالا یادگیری ماشین، نقش به‌سزایی در تقویت شبکه‌های امنیت سایبری خواهد داشت.

۲. انجام پیش‌بینی‌های سرمایه‌گذاری

فناوری‌های مبتنی بر یادگیری ماشین، بینش‌های پیشرفته‌ای از داده‌های بازار ارائه می‌کنند که این بینش جدید به مدیران سرمایه‌گذاری اجازه می‌دهد تا تغییرات خاص بازار را خیلی زودتر از مدل‌های سرمایه‌گذاری سنتی شناسایی کنند.

با سرمایه‌گذاری گسترده شرکت‌های مشهوری مانند JPMorgan، Bank of America و Morgan Stanley در فناوری‌های یادگیری ماشین برای توسعه مشاور سرمایه‌گذاری اتوماتیک، اختلال در صنعت بانکداری سرمایه‌گذاری کاملا مشهود است.

۳. خودکارسازی فرایندها

راه حل‌های مبتنی بر یادگیری ماشین به شرکت‌های مالی این امکان را می‌دهد که کارهای دستی سازمان را با خودکارسازی کارهای تکراری از طریق اتوماسیون فرایند هوشمند برای افزایش بهره‌وری کسب‌وکار جایگزین کنند.

چت‌بات‌ها، اتوماسیون کاغذی، گیمیفیکیشن فرایندها و آموزش کارمندان، نمونه هایی از اتوماسیون فرایند در امور مالی، با استفاده از یادگیری ماشین هستند. این امر به شرکت‌های حوزه مالی امکان می‌دهد تا تجربه مشتری خود را بهبود بخشند، هزینه‌ها را کاهش و خدمات خود را افزایش دهند.

فناوری یادگیری ماشین همچنین می‌تواند به‌راحتی با دسترسی به داده‌ها، رفتارها را تفسیر و الگوهای رفتاری را دنبال کند و تشخیص دهد. از این قابلیت می‌توان به‌راحتی برای سیستم‌های پشتیبانی مشتری استفاده کرد. یادگیری ماشین می‌تواند شبیه به یک انسان واقعی کار کند و پاسخ تمام سوالات منحصربه‌فرد مشتریان را بدهد.

به عنوان مثال می‌توان شرکت Wells Fargo را نام برد که از چت ربات مبتنی بر یادگیری ماشین، بر بستر نرم‌افزار پیام‌رسان Facebook برای برقراری ارتباط موثر با کاربران خود استفاده می‌کند. چت ربات به مشتریان کمک می‌کند تا تمام اطلاعات مورد نیاز خود را در مورد حساب و رمز عبور خود دریافت کنند.

۴. تراکنش‌های امن

الگوریتم‌های یادگیری ماشین در تشخیص تقلب‌های تراکنشی، با توجه به توانایی آنها در تجزیه‌وتحلیل میلیون‌ها نقطه داده که معمولاً توسط انسان‌ها مورد توجه قرار نمی‌گیرند، عالی هستند. این مدل‌ها معمولاً بر مبنای رفتار مشتری در اینترنت و تاریخچه تراکنش‌ها ساخته می‌شوند.

یادگیری ماشین علاوه بر داشتن توانایی شناسایی رفتارهای کلاه‌برداری با دقت بالا، همچنین توانایی شناسایی رفتار حساب‌های کاربری مشکوک، پیش‌بینی و جلوگیری از کلاه‌برداری به صورت آنلاین، به جای شناسایی آنها پس از ارتکاب جرم را نیز دارند.

طبق یک تحقیق، تقریباً به ازای هر یک دلار ازدست‌رفته بر اثر کلاه‌برداری، هزینه بازیابی تحمیل‌شده به مؤسسات مالی نزدیک به ۲٫۹۲ دلار است.

یکی از موفق‌ترین کاربردهای یادگیری ماشین، تشخیص کلاه‌برداری کارت اعتباری است. بانک‌ها مجهز به سیستم‌هایی نظارتی هستند که روی دیتاسِت تاریخچه داده‌های پرداخت، آموزش دیده‌اند. آموزش الگوریتم، اعتبارسنجی و بک‌تست بر مبنای مجموعه‌ای وسیع از داده تراکنش‌های کارت‌های اعتباری انجام شده است. الگوریتم‌های طبقه‌بندی مبتنی بر یادگیری ماشین می‌توانند به‌راحتی رویدادها را به عنوان تقلب و غیرتقلب برچسب‌گذاری کنند تا تراکنش‌های جعلی به صورت آنلاین متوقف شوند.

۵. مدیریت ریسک

با استفاده از تکنیک‌های یادگیری ماشین، بانک‌ها و سایر موسسات مالی با تجزیه‌وتحلیل حجم عظیمی از منابع داده‌ای، می‌توانند سطح ریسک را به میزان قابل توجهی کاهش دهند. برخلاف روش‌های سنتی که معمولاً به اطلاعات ضروری مانند امتیاز اعتباری محدود می‌شوند، یادگیری ماشین می‌تواند حجم قابل توجهی از اطلاعات شخصی افراد را برای کاهش ریسک تجزیه‌وتحلیل کند.

بینش‌های مختلفی که توسط فناوری یادگیری ماشین جمع‌آوری می‌شود، به سازمان‌های خدمات مالی و بانکی، هوشمندی عملیاتی برای کمک به تصمیم‌گیری‌های بعدی را ارائه می‌دهد.

به عنوان مثال از کاربردهای مدیریت ریسک می‌توان از برنامه یادگیری ماشینی نام برد که با مراجعه به منابع مختلف داده‌ای و محاسبه امتیاز ریسک برای مشتریانی که درخواست وام می‌کنند، به سازمان‌ها در تصمیم‌گیری برای اعطا یا عدم اعطای وام کمک می‌دهند.

الگوریتم‌های یادگیری ماشین می‌توانند به‌راحتی مشتریانی را که در معرض خطر عدم بازپرداخت وام‌هایشان هستند، پیش‌بینی و به شرکت‌ها کمک کنند که شرایط را برای هر مشتری بازنگری یا تنظیم کنند.

۶. معاملات الگوریتمی

یادگیری ماشین در معاملات الگوریتمی نمونه عالی دیگری از استفاده در صنعت مالی است. معاملات الگوریتمی (AT) به یک نیروی مسلط در بازارهای مالی جهانی تبدیل شده است.

راه‌حل‌ها و مدل‌های مبتنی بر یادگیری ماشین به شرکت‌های تجاری این امکان را می‌دهند تا با نظارت دقیق بر نتایج و اخبار معاملاتی که می‌توانند قیمت سهام‌ها را بالا یا پایین کنند، به صورت آنلاین، الگوهایی را شناسایی و تصمیمات معاملاتی بهتری اتخاذ کنند.

الگوریتم‌های یادگیری ماشین همچنین می‌توانند صدها منبع داده را به طور همزمان تجزیه‌وتحلیل کنند و به معامله‌گران، برتری متمایزی نسبت به میانگین بازار ارائه دهند.

برخی از مزایای دیگر معاملات الگوریتمی عبارتند از:
۱- افزایش دقت و کاهش احتمال اشتباه
۲- انجام معاملاتی با بهترین قیمت ممکن
۳- احتمال کاهش خطاهای انسانی به میزان قابل توجهی
۴- بررسی خودکار و همزمان چندین شرایط بازار

۷. مشاوره مالی

برنامه‌های مدیریت بودجه مختلفی وجود دارند که بر پایه یادگیری ماشین طراحی شده‌اند و می‌توانند مزایای مشاوره و راهنمایی مالی بسیار تخصصی و هدفمند را به مشتریان ارائه دهند.

الگوریتم‌های یادگیری ماشینی نه تنها به مشتریان اجازه می‌دهند تا با استفاده از این برنامه‌ها هزینه‌های خود را به صورت روزانه بررسی کنند، بلکه به آنها کمک می‌کند تا این داده‌ها را برای شناسایی الگوهای مخارج خود تجزیه‌وتحلیل و سپس نواحی‌ای را که می‌توانند در هزینه‌ها صرفه‌جویی و پس‌انداز کنند، شناسایی کنند.

یکی از دیگر ترندهای به‌سرعت در حال ظهور در این زمینه، Robo-Advisorsها هستند. آنها مانند مشاوران معمولی کار می‌کنند و به طور خاص سرمایه‌گذارانی با منابع محدود، افراد و مشاغل کوچک تا متوسط را هدف قرار می‌دهند که مایل به مدیریت سرمایه خود هستند.

این ربات‌های مشاور مبتنی بر یادگیری ماشین، توانایی دارند که از تکنیک‌های سنتی پردازش داده برای ایجاد پورتفولیوهای مالی و راه‌حل‌هایی مانند تجارت، سرمایه‌گذاری، برنامه‌های بازنشستگی و غیره برای ارائه مشاوره به کاربران خود استفاده کنند.

۸. مدیریت داده‌های مشتری

وقتی صحبت از بانک‌ها و مؤسسات مالی می‌شود، داده‌ها حیاتی‌ترین منبع هستند که مدیریت کارآمد آنها عامل رشد و موفقیت این کسب‌وکارهاست.

حجم عظیم و تنوع ساختاری داده‌های مالی که شامل ارتباطات تلفن همراه، فعالیت‌های رسانه‌های اجتماعی و جزئیات تراکنش‌ها و داده‌های بازار است، باعث می‌شود پردازش دستی این داده‌های حجیم حتی برای متخصصان مالی، چالش بزرگی باشد.

ادغام تکنیک‌های یادگیری ماشین برای مدیریت چنین حجم زیادی از داده‌ها می‌تواند هم کارایی فرایند و هم سود استخراج اطلاعات واقعی از داده‌ها را به همراه داشته باشد. ابزارهای هوش مصنوعی و یادگیری ماشین مانند تجزیه‌وتحلیل داده‌ها، داده‌کاوی و پردازش زبان طبیعی، به دریافت بینش ارزشمندی از داده‌ها برای سودآوری بهتر کسب‌وکارها کمک می‌کنند.

یک مثال عالی می‌تواند الگوریتم‌های یادگیری ماشینی باشد که به منظور تجزیه‌وتحلیل

تأثیر تحولات بازار و روندهای مالی خاص، از داده‌های مالی مشتریان استفاده می‌کند.

۹. تصمیم‌گیری

بانک‌ها و موسسات مالی می‌توانند از الگوریتم‌های یادگیری ماشین برای تجزیه‌وتحلیل داده‌های ساختاریافته و بدون ساختار استفاده کنند. به عنوان مثال از درخواست‌های مشتریان، تعاملات رسانه‌های اجتماعی با یکدیگر و فرایندهای مختلف تجاری داخلی شرکت، با کمک یادگیری ماشین، روندهایی کشف می‌شود که هم می‌تواند برای سودآوری مفید باشد و هم نشان‌دهنده ریسک سرمایه‌گذاری. کشف روندها می‌تواند خدمات خاصی باشد که به تصمیم‌گیری دقیق مشتریان کمک ویژه‌ای می‌کند.

۱۰- بهبود سطح خدمات مشتری

با استفاده از یک ربات چت هوشمند، مشتریان می‌توانند تمام سوالات خود را درمورد هزینه‌های ماهانه، واجد شرایط‌بودن برای اخذ وام، طرح‌های بیمه مقرون‌به‌صرفه و موارد دیگر مطرح کنند و پاسخ بگیرند.

علاوه بر این، چندین برنامه کاربردی مبتنی بر یادگیری ماشین وجود دارد که وقتی به یک سیستم پرداخت متصل می‌شوند، می‌توانند حساب‌ها را تجزیه‌وتحلیل کنند و به مشتریان کمک کنند پول خود را پس‌انداز کرده و رشد دهند.

الگوریتم‌های پیچیده یادگیری ماشین را می‌توان برای تجزیه‌وتحلیل رفتار کاربر و توسعه پیشنهادات سفارشی استفاده کرد. به عنوان مثال، مشتری که به دنبال سرمایه‌گذاری در یک طرح مالی است، می‌تواند پس از تجزیه‌وتحلیل الگوریتم یادگیری ماشین از وضعیت مالی موجود او، از یک پیشنهاد سرمایه‌گذاری شخصی بهره‌مند شود.

۱۱. برنامه حفظ مشتری

شرکت‌های کارت‌های اعتباری می‌توانند از فناوری یادگیری ماشین برای پیش‌بینی مشتریان در معرض خطر استفاده کنند و اقدامات لازم را به منظور حفظ مشتریان خود انجام دهند.

این نرم‌افزارها بر اساس داده‌های جمعیت‌شناختی کاربر و فعالیت تراکنشی او، به‌راحتی می‌توانند رفتار کاربر را پیش‌بینی و پیشنهاداتی را به طور خاص برای این مشتریان طراحی کنند.

این نرم‌افزار، شامل یک مدل طبقه‌بندی باینری پیش‌بینی‌کننده برای یافتن مشتریان در معرض خطر است و به دنبال آن از یک مدل توصیه‌گر برای تعیین بهترین پیشنهادات کارت استفاده می‌کند که می‌تواند به حفظ این مشتریان کمک کند.

۱۲. بازاریابی

توانایی مدل‌های هوش مصنوعی و یادگیری ماشین برای پیش‌بینی‌های دقیق بر اساس رفتار گذشته، آنها را به یک ابزار بازاریابی عالی تبدیل می‌کند. از تجزیه‌وتحلیل

استفاده از برنامه تلفن همراه، فعالیت‌های وب و پاسخ‌ها به کمپین‌های تبلیغاتی قبلی، الگوریتم‌های یادگیری ماشینی می‌توانند به ایجاد یک استراتژی بازاریابی قوی برای شرکت‌های مالی کمک کنند.

چشم‌انداز آینده یادگیری ماشین در حوزه مالی

در حالی که برخی از کاربردهای یادگیری ماشینی در بانکداری و امور مالی به‌وضوح شناخته شده و قابل مشاهده هستند، مانند چت‌بات‌ها و برنامه‌های بانکداری تلفن همراه، الگوریتم‌ها و فناوری یادگیری ماشین، به‌تدریج برای برنامه‌های نوآورانه آینده نیز، با کمک ترسیم دقیق داده‌های تاریخی مشتریان مورد استفاده قرار می‌گیرند و آینده آنها را پیش‌بینی می‌کنند.

جدا از موارد استفاده تثبیت‌شده یادگیری ماشین در امور مالی، همان‌طور که در بخش بالا مورد بحث قرار گرفت، چندین برنامه کاربردی امیدوارکننده دیگر وجود دارد که فناوری یادگیری ماشین می‌تواند در آینده ارائه دهد. در حالی که تعداد کمی از این برنامه ها امروزه کاربردهای نسبتاً فعالی دارند، برخی دیگر هنوز در مرحله اولیه و آزمایشی هستند. در ادامه برخی از کاربردهای آینده یادگیری ماشین و هوش تجاری را مورد بررسی قرار می دهیم:

توصیه و فروش محصولات مالی مختلف

اگرچه امروزه نیز کاربردهای مختلفی از فروش یا توصیه‌های خودکار محصول مالی وجود دارد، بسیاری از آنها سیستم‌های مبتنی بر قوانین (به جای یادگیری ماشین) هستند که در آنها، داده‌ها هنوز از طریق منابع دستی عبور می‌کنند تا بتوانند معاملات یا سرمایه‌گذاری‌ها را به مشتریان توصیه کنند.

در آینده شاهد استفاده فعالانه سایت‌های توصیه‌گر بیمه از فناوری‌های یادگیری ماشین و هوش مصنوعی به منظور پیشنهاد بیمه‌نامه (خانه یا وسیله نقلیه) اختصاصی به مشتریان خواهیم بود. علاوه بر این، یک روند جالب و سریعی که در آینده شاهد آن خواهیم بود این است که ربات مشاورها، خدمات مشاوره‌ای قابل اعتمادتری را در حوزه مالی مانند مدیریت سبد و دارایی‌ها به مشتریان ارائه خواهند داد.

افزایش امنیت

امنیت داده‌ها در بانکداری و امور مالی بسیار حیاتی است. با آنلاین‌شدن تمامی خدمات، حفظ امنیت اطلاعات کاربران یعنی نام کاربری، کلمه عبور و سوالات امنیتی، به یک چالش روزافزون شرکت‌ها تبدیل شده است. ممکن است در چند سال آینده،

تغییر چشم‌گیری در این حوزه را مشاهده کنیم که کلمه عبور، نام کاربری و سوالات امنیتی دیگر، روشی برای تامین امنیت کاربر نباشد.
برنامه‌های کاربردی یادگیری ماشین، امنیت آینده را در صنعت با به‌کارگیری تشخیص صدا، تشخیص صورت یا سایر داده‌های بیومتریک مشابه تامین خواهند کرد.
Stripe، PayPal، Payoneer، Adyen و Skrill برخی از شرکت‌هایی هستند که به‌شدت در یادگیری ماشین‌های امنیتی سرمایه‌گذاری کرده‌اند.

تجزیه‌وتحلیل احساسات مشتری

مدل‌های یادگیری ماشین می‌توانند کمک بزرگی به شرکت‌های حوزه مالی در تحلیل روندهای فعلی بازار، پیش‌بینی تغییرات و استفاده هر مشتری از رسانه‌های اجتماعی بکند.
از آنجایی که عوامل انسانی در درجه اول بازار سهام را هدایت می‌کنند، کسب‌وکارها باید به طور مداوم از فعالیت های مالی کاربران یادگیری داشته باشند. علاوه بر این، تجزیه‌وتحلیل احساسات مصرف‌کننده می‌تواند اطلاعات فعلی را درمورد انواع مختلف تحولات تجاری و اقتصادی تکمیل کند.

خدمات بهتر به مشتری

تعداد روزافزون موسسات مالی در حال حاضر، اولویت‌بندی مشتری را به دلایل واضح تعیین می‌کند. به غیر از کمک به آنها بهبود نرخ نگهداری، کمک می‌کند تا رفتار کاربر، نگرانی‌ها و نیازهای آنها را درک کنند. یک نمونه عالی از این مورد، Chatbots مالی مورد استفاده برای ارتباطات فوری با مشتری است.
آینده به این صورت خواهد بود که دستیارهای چت فراوانی برای تعامل با مشتریان اختصاص داده خواهد شد و موتورهای پردازش طبیعی ایجاد می‌شود تا بتوانند تعامل سریع از طریق پرس‌وجو را فراهم کنند.
در حالی که این نوع تجربه تخصصی Chatbots امروزه در صنعت بانکی یا مالی حضور چشمگیری ندارد، اما احتمال بسیار زیادی برای پدیدآمدن آن در آینده وجود دارد. این Chatbots یک برنامه کاربردی و از یادگیری ماشین است. از امور مالی فراتر می‌رود و احتمالا در انواع زمینه های مختلف و بسیاری از صنایع دیده خواهد شد.

یادگیری ماشین در امور مالی؛ چه اتفاقی می‌افتد؟

امروزه یادگیری ماشین نقش مهمی در جنبه‌های مختلف اکوسیستم مالی بازی می‌کند؛ از مدیریت دارایی‌ها، ارزیابی ریسک، ارائه مشاوره سرمایه‌گذاری، برخورد با تقلب در امور مالی تا احراز هویت سندها.

در حالی که الگوریتم‌های یادگیری همواره در حال انجام تعداد زیادی تسک در سازمان هستند، به طور مداوم از داده‌های ورودی به الگوریتم، یاد می‌گیرند و شکاف بین دنیای واقعی و سیستم هوشمند کاملا اتوماتیک، در گذر زمان کمتر می‌شود.
برای بسیاری از شرکت‌های مالی، نیاز همکاری با شرکت‌های باتجربه‌ای که خدمات توسعه و راه‌اندازی سامانه‌های یادگیری ماشین و هوش مصنوعی را ارائه می‌دهند، ایجاد خواهد شد.
همکاری با این شرکت‌ها باعث می‌شود شما با تمرکز بر منابع داده‌ای موجود در سازمان و کسب‌وکار مرتبط به آن، به طور دقیق خروجی مورد نیاز از هر منبع داده را ترسیم کنید و با تلفیق خروجی‌ها به نتایج دلخواه خود برسید.

چهار روش تقلب رایج در دنیا در سال ۲۰۲۰

فاطمه مصلحی
برنامه‌نویس راهکارهای تشخیص تقلب داتین

۱ شبیه‌سازی کارت — Card Cloning

شبیه‌سازی کارت، یا «اسکیمینگ»، کپی‌کردن اطلاعات کارت اعتباری یا بدهی سرقت‌شده در یک کارت جدید است.

۲ سفارش/پرداخت با سرعت بالا — High Speed Ordering/ Spending

کلاه‌برداران اغلب با استفاده از حملات ربات، سفارش‌های پرسرعت را انجام می‌دهند. ربات‌ها می‌توانند صدها بار در چند دقیقه کلیک کنند. برخی از حملات ربات‌ها می‌توانند تا چند ساعت طول بکشند.

۳ مشاغل پرخطر — High Risk Merchant Category Code

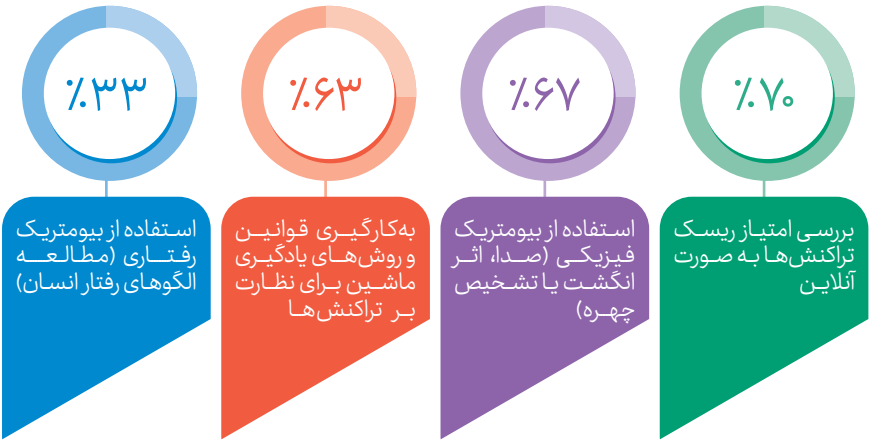
وب‌سایت مشاغل پرخطر نظیر سایت‌های شرط‌بندی و قمار و سایت‌های ارائه‌دهنده خدمات مسافرتی

۴ جعل هویت و حساب — Account Takeover (ATO)

جعل حساب کاربری، زمانی است که یک کلاه‌بردار به حساب یک مشتری معتبر دسترسی پیدا می‌کند.

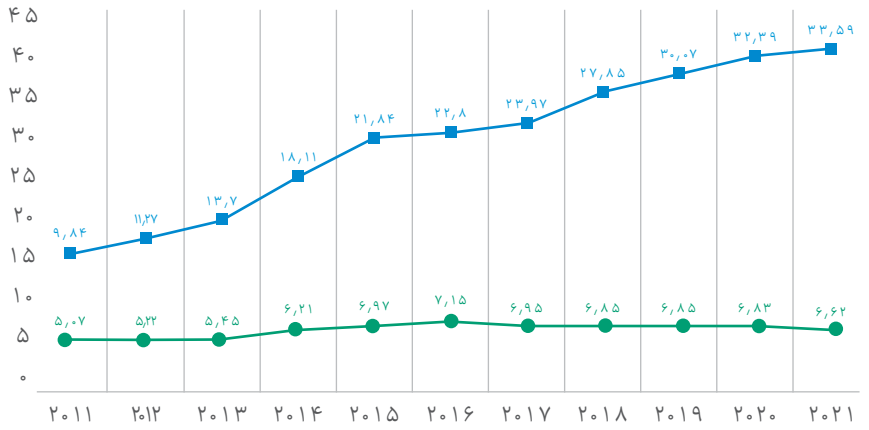
Ref: feedzai.com

بانک‌های جهانی چگونه با تقلب مقابله می‌کنند؟



Ref: KPMG/ Global Banking Fraud Survey

مبلغ زیان حاصل از تقلب



Ref: Nilson report

نگاهی به آخرین گزارش اتحادیه تجاری نظام بانکی انگلیس[1] از انواع کلاه‌برداری‌های بانکی در سال ۲۰۲۰

آرمین منتظری
روزنامه‌نگار

خانواده‌ها و مشاغل در دوران پاندمی کرونا با مشکل مواجه شدند اما در این میان، باندهای جنایتکار جرایم اقتصادی به‌سرعت از این پاندمی استفاده کرده و روش‌های جدید کلاه‌برداری را ابداع کردند. این روش‌های کلاه‌برداری، شامل جعل هویت نیز است که این مورد، ترس مردم را موجب می‌شود. روشی که طی آن کلاه‌برداران وانمود می‌کنند از سازمان‌های قابل اعتمادی مانند وزارت بهداشت، بیمارستان یا ادارات دولتی هستند و سعی می‌کنند از این طریق دست به کلاه‌برداری بزنند.

علاوه بر این، کلاه‌برداران با توجه به افزایش خرید آنلاین و دورکاری در دوران پاندمی، با جعل هویت شرکت‌های تحویل کالا، جعل پلتفرم‌های تجارت الکترونیک یا ارائه‌دهندگان پهنای باند، دست به کلاه‌برداری زدند. علاوه بر این، مجرمان با ارسال آگهی‌های جعلی در وب‌سایت‌های شغلی و رسانه‌های اجتماعی، کلاه‌برداری کرده‌اند.

1.UK Finance

اگر بخواهیم کمی واضح‌تر سخن بگوییم باید اذعان کنیم که این کلاه‌برداران صرفا افراد فرصت‌طلب نیستند بلکه آنها مجرمانی سازمان‌یافته و بی‌رحم هستند که از تکنیک‌های پیچیده برای فریب‌دادن افراد استفاده می‌کنند تا به اطلاعات شخصی یا مالی آنها دست یابند.

باندهای جنایت‌کار درگیر این شیوه‌های کلاه‌برداری، از عواید حاصل از این اقدامات، برای تأمین مالی سایر فعالیت‌های مضر و غیرقانونی مانند برده‌داری انسان یا قاچاق مواد مخدر استفاده می‌کنند که باعث رنج و آسیب‌های بی‌حدوحصر بر جامعه می‌شود. بنابراین وظیفه همه ما، در بخش خصوصی، مجریان قانون و دولت این است که با هم برای مقابله با این تهدید تلاش کنیم.

کارکنان بانک‌ها در دوران پاندمی کرونا در خط مقدم محافظت از مشتریان در برابر کلاه‌برداری و کمک به پلیس برای دستگیری مجرمان، مسئول هستند و در این زمینه تلاش کرده‌اند. بر اساس گزارش UK Finance، در سال ۲۰۲۰، بانک‌ها و مجریان قانون، یک میلیارد و ۶۰۰ میلیون پوند کلاه‌برداری غیرمجاز را در سال ۲۰۲۰ متوقف کردند. یعنی از هر ۱۰ پوند مبلغ کلاه‌برداری‌شده، حدود هفت پوند آنها متوقف شده است.

آنچه در ذیل می‌خوانید گزارش سال ۲۰۲۰ نهاد مالی UK Finance درباره روش‌های کلاه‌برداری بانکی و روش‌های مقابله با آن است:

کلاه‌برداران از روش‌های جدیدی برای کلاه‌برداری استفاده می‌کنند؛ از جمله کلاه‌برداری با استفاده از بهینه‌سازی موتورهای جست‌وجو و ایجاد وب‌سایت‌های جعلی برای هدایت مشتریان به وب‌سایت‌های کلاه‌برداری. معمولاً به مشتریان گفته می‌شود که فرم‌های آنلاین را در این وب‌سایت‌های جعلی پر کنند که از این طریق، کلاه‌برداران اطلاعات مالی آنها را به دست می‌آورند.

تماس از طرف شخصی که هویت یک شرکت سرمایه‌گذاری یا کارگزار واقعی را جعل کرده یکی دیگر از روش‌هاست. مجرمان همچنین گاهی اوقات اسناد جعلی را که در ظاهر کاملا طبیعی است ارسال می‌کنند تا کلاه‌برداری خود را طبیعی جلوه دهند یا دسترسی به پورتال‌های آنلاینی را فراهم می‌کنند که ادعا می‌کنند به قربانی اجازه می‌دهد بر عملکرد سرمایه‌گذاری خود نظارت داشته باشد.

مجرمان همچنین از رسانه‌های اجتماعی و خدمات پیام‌رسانی دیجیتال برای ترویج فرصت‌های سرمایه‌گذاری جعلی، از جمله در تجارت فارکس و ارزهای دیجیتال استفاده می‌کنند که مورد دوم با موفقیت و هجوم مردم به بازار رمزارزهایی نظیر بیت‌کوین و اتریوم، برای کلاه‌برداران، بازار پرسودی است.

البته پاندمی کرونا هم در این میان به کلاه‌برداران کمک کرد، چراکه محدودیت هایی نظیر قرنطینه و فاصله‌گذاری اجتماعی منجر به افزایش قابل توجه استفاده مردم از خدمات

آنلاین شد و به این ترتیب فرصتی را برای مجرمان فراهم کرد. در واقع این روزها هر کلاه‌برداری به نوعی از خدمات آنلاین سوءاستفاده می‌کند.
آخرین ارقام کلاه‌برداری نشان می‌دهد که افزایش قابل توجهی در کلاه‌برداری‌های اینترنتی و بانکداری تلفن همراه در سال ۲۰۲۰ رخ داده که تا حدودی ناشی از افزایش استفاده از این خدمات بوده است. ارقام مربوط به سال ۲۰۱۹ نشان می‌دهد که ۸۱ درصد از جمعیت بزرگسال در انگلیس حداقل از یک شکل بانکداری از راه دور استفاده می‌کنند و این احتمال وجود دارد که این میزان بالای استفاده، ناشی از پاندمی کرونا باشد. آسیب‌های ناشی از این استفاده زیاد نیز افزایش یافته، به طوری که کلاه‌برداران به طور فزاینده‌ای قربانیان را به طور مستقیم از طریق ارسال ایمیل‌های فیشینگ هدف قرار می‌دهند و از تکنیک‌های مهندسی اجتماعی برای ارائه رمز عبور و واردکردن جزئیات حساب بانکی‌شان استفاده می‌کنند.

واکنش نظام بانکداری به کلاه‌برداری‌ها

صنعت بانکداری و مالی انگلیس به‌شدت در تلاش است تا از مشتریان در برابر کلاه‌برداری محافظت کند. در عین حال با مجریان قانون نیز همکاری می‌کند تا باندهای جنایتکار مسئول را دستگیر و تحت پیگرد قانونی قرار دهد. رویکرد صنعت بانکداری انگلیس در مواجهه با کلاه‌برداری‌های بانکی به شرح زیر است:
۱- سرمایه‌گذاری در طراحی و ساخت سیستم‌های امنیتی پیشرفته برای محافظت از مشتریان در برابر تقلب، از جمله تجزیه‌وتحلیل معاملات بلادرنگ. این صنعت در سال ۲۰۲۰ از یک میلیارد و ۶۰۰ میلیون پوند کلاه‌برداری غیرمجاز جلوگیری کرد.
۲- همکاری با دولت و مجریان قانون برای تعیین اولویت‌های استراتژیک، بهبود پاسخ‌گویی و هماهنگی از طریق هیئت راهبردی جرایم اقتصادی، به ریاست مشترک وزیر کشور و نخست‌وزیر.
۳- هماهنگی برای پاسخ مشترک به جرائم اقتصادی و به‌اشتراک‌گذاری اطلاعات تهدیدات نوظهور با مجریان قانون، ادارات دولتی و تنظیم‌کنندگان مقررات از طریق مرکز ملی جرائم اقتصادی.
۴- UK Finance با دولت، مجریان قانون و تنظیم‌کنندگان مقررات همکاری می‌کند تا یک برنامه اقدام پیشرفته‌تر برای مبارزه با کلاه‌برداری بانکی ایجاد کند.
۵- به‌اشتراک‌گذاری اطلاعات در سراسر صنعت بانکداری و مالی درمورد تهدیدهای نوظهور، نقض داده‌ها و جزئیات کارت‌های بانکی به‌خطرافتاده از طریق واحد اطلاعات مالی بریتانیا. در سال ۲۰۲۰، تعداد دو میلیون و ۱۰۰ هزار شماره کارت بانکی به‌خطرافتاده از طریق شرکای استراتژیک مجری قانون دریافت و منتشر شد تا صادرکنندگان کارت‌های

بانکی بتوانند اقدامات احتیاطی لازم را برای محافظت از مشتریان انجام دهند.
۶- این صنعت با مجری قانون همکاری می‌کند تا از طریق ابتکاراتی مانند پروتکل بانکی، کلاه‌برداری را متوقف کند. این طرح به کارکنان شعب بانک‌ها اجازه می‌دهد زمانی که فکر می‌کنند از مشتری کلاه‌برداری می‌شود، به پلیس هشدار دهند. این طرح ۴۵ میلیون و ۳۰۰ هزار پوند کلاه‌برداری را متوقف کرد و منجر به دستگیری ۲۰۰ نفر در سال ۲۰۲۰ شد. از زمان اجرای این طرح در سال ۲۰۱۶ نیز ۸۴۳ نفر شده‌اند. این طرح در حال حاضر در حوزه بانکداری تلفنی و آنلاین در حال گسترش است. این دو حوزه نیز به طور ویژه برای مشتریانی که به دلیل محدودیت‌های قرنطینه ویروس کرونا نتوانسته‌اند به شعبه خود مراجعه کنند، بسیار مهم بوده است.
۷- تأمین مالی کامل یک واحد پلیس متخصص «واحد اختصاصی کارت بانکی و جرائم پرداخت» که با گروه‌های جنایتکار سازمان‌یافته مسئول کلاه‌برداری‌های مالی و کلاه‌برداری مقابله می‌کند. این واحد در طول سال ۲۰۲۰ از تقلب ۲۰ میلیون پوندی جلوگیری و ۱۲۲ مظنون کلاه‌بردار را دستگیر کرد. همچنین فعالیت‌های اجرایی را علیه مجرمان به اجرا گذاشت. این واحد همچنین با پلتفرم‌های رسانه‌های اجتماعی برای حذف بیش از ۷۰۰ حساب مرتبط با فعالیت‌های کلاه‌برداری در سال ۲۰۲۰ کار کرده که بیش از ۲۵۰ نفر از آنها استخدام‌کننده پول بودند.
۸- همکاری با ارائه‌دهندگان پیام‌های متنی و مجریان قانون برای مسدودکردن پیام‌های متنی کلاه‌برداری از جمله پیام‌هایی که از بحران پاندمی سوءاستفاده می‌کنند. در این مسیر، هزار و ۸۷ شناسه فرستنده غیرمجاز برای جلوگیری از ارسال پیام‌های متنی کلاه‌برداری با تقلید از سازمان‌های مورد اعتماد مسدود شده‌اند.
۹- همکاری با رگولاتور Ofcom برای مقابله با جعل اعداد، از جمله از طریق ایجاد یک لیست. آفکام اعلام کرده این کار به موفقیت‌های چشم‌گیری در جلوگیری از جعل شماره تلفن سازمان‌های مورد اعتماد منجر شده است.
۱۰- همکاری با Cifas در کمپین «گول نخورید»، که هدف آن اطلاع‌رسانی به دانش‌آموزان و جوانان درمورد خطرات ارائه اطلاعات بانکی آنهاست.
۱۱- همکاری با Pay.UK برای پیاده‌سازی یک فناوری که به ردیابی پرداخت‌های مشکوک و شناسایی حساب‌های پولی کمک می‌کند.
۱۲- همکاری با Pay.UK برای اجرای Confirmation of Payee، یک سرویس بررسی نام حساب که به جلوگیری از کلاه‌برداری‌های مجاز پرداخت فشاری کمک می‌کند. از ۳۰ ژوئن ۲۰۲۰، این اقدام به طور کامل توسط شش گروه بانکی بزرگ بریتانیا اجرا شده و از آن زمان به بعد گسترش یافته و بیش از ده‌ها ارائه‌دهنده پرداخت را پوشش می‌دهد. بیش از یک میلیون درخواست تائیدگیرنده هر روز انجام می‌شود که بیش از ۹۰ درصد از حجم

پرداخت‌های سریع‌تر را پوشش می‌دهد. انتظار می‌رود ارائه‌دهندگان بیشتری در سال ۲۰۲۱ ثبت نام کنند.
۱۳- کمک به مشتریان در برابر کلاه‌برداری و شناسایی نشانه‌های کلاه‌برداری.

انواع کلاه‌برداری‌های بانکی در سال ۲۰۲۰

کلاه‌برداری غیرمجاز از دبیت‌کارت‌ها، کارت‌های اعتباری و سایر موارد

خسارات ناشی از کلاه‌برداری در کارت‌های بانکی صادرشده در بریتانیا در سال ۲۰۲۰ به ۵۷۴ میلیون و دویست هزار پوند رسید که نسبت به ۶۲۰ میلیون پوند در سال ۲۰۱۹، هفت درصد کاهش داشت. داده‌های مربوط به کل هزینه‌های مربوط به همه کارت‌های بدهی و اعتباری هنوز در دسترس نیست اما گزارش برای منعکس‌کردن این ارقام به‌روزرسانی خواهد شد.
در سال ۲۰۲۰، مجموعاً ۹۸۳ میلیون پوند کلاه‌برداری کارت‌های بانکی و شرکت‌های صادرکننده دبیت کارت متوقف شد که کاهش دو درصدی نسبت به سال ۲۰۱۹ را نشان می‌دهد. این رقم معادل ۶٫۳۱ پوند در هر ۱۰ پوند تلاش برای کلاه‌برداری از کارت است.
این ارقام کلاه‌برداری در کارت‌های نقدی، اعتباری، شارژی و فقط کارت‌های خودپرداز صادرشده در بریتانیا را پوشش می‌دهد. ضررهای ناشی از کلاه‌برداری کارت نقدی به پنج دسته تقسیم می‌شود؛ خرید از راه دور، کارت جعلی، کارت گم‌شده و دزدیده‌شده، کارت دریافت‌نشده و سرقت شناسه کارت. تجزیه‌وتحلیل صنعت نشان می‌دهد که بانک‌ها و شرکت‌های صادرکننده کارت در بیش از ۹۸ درصد موارد به مشتریان بازپرداخت می‌کنند.
نظام بانکداری انگلیس از طرق زیر با کلاه‌برداری کارت‌های نقدی مبارزه می‌کند:
۱- سرمایه‌گذاری در سیستم‌های امنیتی پیشرفته برای محافظت از مشتریان، از جمله تجزیه‌وتحلیل معاملات بلادرنگ و بیومتریک‌های رفتاری در دستگاه‌ها. احراز هویت قوی مشتری (SCA) برای پرداخت‌های آنلاین با ارزش بالاتر.
۲- توسعه ابزارهای تشخیص تقلب برای خرده‌فروشان، مانند فناوری 3D Secure که از خرید آنلاین کارت محافظت می‌کند.
۳- شناسایی سریع و ایمن جزئیات کارت به‌خطرافتاده از طریق مرکز اطلاعاتی UK Finance به طوری که صادرکنندگان کارت بتوانند محافظت‌هایی را اعمال کنند.
۴- همکاری با دولت و مجریان قانون در گروه ویژه تقلب برای استفاده از منابع جمعی برای سرکوب کلاه‌برداری مالی.
۵- تأمین مالی یک واحد پلیس تخصصی، «واحد جرائم اختصاصی کارت و پرداخت» (DCPCU)، که با باندهای جنایتکار سازمان‌یافته مسئول کلاه‌برداری‌های مالی مقابله می‌کند.


HSBC UK
Welcome
to Moorgate
together
Premier

کلاه‌برداری خرید از راه دور بدون استفاده از کارت از طریق اینترنت، تلفن و سفارش پستی

این کلاه‌برداری زمانی اتفاق می‌افتد که مجرم از اطلاعات کارت سرقت‌شده برای خرید چیزی از طریق اینترنت، تلفن یا پست استفاده کند. به طور کلی، تقلب در خرید از راه دور در سال ۲۰۲۰ به ۴۵۲ میلیون پوند کاهش یافت، که در مقایسه با سال ۲۰۱۹، چهار درصد کاهش داشت. تقلب آنلاین علیه خرده‌فروشان بریتانیا در مجموع ۲۶۲ میلیون پوند در سال ۲۰۲۰ تخمین زده شد که ۹ درصد نسبت به سال قبل افزایش داشت. کلاه‌برداری از طریق پست یا تلفن علیه خرده‌فروشان مستقر در بریتانیا بالغ بر ۶۴ میلیون پوند است که در مقایسه با سال ۲۰۱۹ کاهش ۲۸ درصدی را نشان می‌دهد.

اطلاعات نشان می‌دهد که کلاه‌برداری خرید از راه دور عمدتاً توسط مجرمانی انجام می‌شود که از جزئیات کارت به‌دست‌آمده و از سرقت داده‌ها، مانند نقض داده‌های شخص ثالث و از طریق ایمیل‌های فیشینگ و پیام‌های متنی استفاده می‌کنند. این شامل کلاه‌برداری‌هایی می‌شود که با جعل هویت سازمان‌های مورد اعتماد مانند دولت و وزارت بهداشت در زمان پاندمی کرونا، انجام شده است. به عنوان مثال از مردم می‌خواهند مشخصات کارت خود را برای رزرو واکسن کووید-۱۹ وارد کنند.

مجرمان همچنین از پروفایل‌های رسانه‌های اجتماعی برای تبلیغ فروش کالاهای تخفیف‌خورده به مصرف‌کنندگان استفاده می‌کنند. هنگامی که یک مشتری محصول را خریداری می‌کند، مجرم از جزئیات کارت سرقت‌شده برای خرید همان کالا از یک منبع قانونی استفاده می‌کند و پرداخت را از مشتری پنهان نگاه می‌دارد.

مجرمان به استفاده از اسکیمرهای دیجیتال برای سرقت داده‌های کارت از مشتریان، هنگام خرید آنلاین ادامه می‌دهند. در یک حمله اسکیمینگ دیجیتال معمولی، مجرمان کدهای مخرب را به آن اضافه می‌کنند. وب‌سایت‌های خرده‌فروش آنلاینی هم هستند که اطلاعات حساس از جمله جزئیات کارت را در مرحله تسویه حساب سرقت می‌کنند. سپس این اطلاعات به دامنه‌ای ارسال می‌شود که توسط مجرمان کنترل می‌شود و از آن برای ارتکاب کلاه‌برداری خرید از راه دور استفاده می‌کنند. این حملات نشان می‌دهد که حفظ تدابیر امنیتی قوی توسط خرده‌فروشان آنلاین، از جمله اطمینان‌یافتن از به‌روزرسانی منظم پلتفرم‌های پرداخت با جدیدترین نرم‌افزارها، تا چه اندازه اهمیت دارد.

نظام بانکی انگلیس در حال کار روی اجرای مرحله‌ای از احراز هویت قوی مشتری است، قوانین جدیدی که با هدف کاهش کلاه‌برداری از طریق تائید هویت مشتری در هنگام خرید آنلاین با ارزش بالاتر انجام می‌شود.

چگونه از کلاه‌برداری خرید از راه دور در امان بمانیم؟

• به پیشنهادات یا قیمت‌های خیلی خوب مشکوک باشید.
• از روش پرداخت امنی که توسط خرده‌فروشان آنلاین و سایت‌های حراج معتبر توصیه می‌شود، استفاده کنید.
• در صورت امکان، هنگام خریدهای بیش از ۱۰۰ پوند و حداکثر ۳۰ هزار پوند، از کارت اعتباری استفاده کنید زیرا طبق بخش ۷۵ قانون مصرف‌کننده کارت اعتباری، از شما محافظت می‌شود.
• برای بررسی واقعی‌بودن وب‌سایت‌ها و فروشندگان، نظرات آنلاین را بخوانید و بخواهید اقلام با ارزش بالا را شخصاً یا از طریق لینک ویدئویی مشاهده کنید. همچنین برای اطمینان از مالکیت فروشنده، کپی‌هایی از اسناد مربوطه را دریافت کنید.
• اقلام ساخته‌شده توسط یک برند بزرگ را از لیست فروشندگان مجاز فهرست‌شده در وب‌سایت رسمی آنها خریداری کنید.
• همیشه با تایپ‌کردن در مرورگر وب به وب‌سایتی که از آن خرید می‌کنید دسترسی داشته باشید و مراقب کلیک‌کردن روی پیوندهای موجود در ایمیل‌های ناخواسته باشید.
• همیشه مطمئن شوید که روی دکمه «خروج» از وب‌سایت‌ها کلیک می‌کنید.
• اگر به دنبال یک حیوان خانگی هستید، آن را مستقیماً از یک پرورش‌دهنده بخرید یا به جای آن از یک مرکز نجات استفاده کنید.

کلاه‌برداری با استفاده از کارت‌های تقلبی

این کلاه‌برداری زمانی اتفاق می افتد که یک مجرم با استفاده از اطلاعات به‌دست‌آمده از نوار مغناطیسی، یک کارت جعلی ایجاد کند. زیان‌های ناشی از کارت‌های تقلبی در سال ۲۰۲۰ به حدود ۹ میلیون پوند رسید که تقریباً یک سوم (۳۲ درصد) نسبت به سال ۲۰۱۹ کاهش داشت و ۹۵ درصد کمتر از بالاترین میزان گزارش‌شده در سال ۲۰۰۸ (۱۶۹٫۸ میلیون پوند) بود. برای به‌دست‌آوردن اطلاعات مورد نیاز برای ایجاد یک کارت تقلبی، مجرمان معمولاً دستگاه‌های پنهان یا مبدل را به شکاف‌های کارت‌خوان دستگاه‌های خودپرداز و پایانه‌های پرداخت بدون مراقبت (UPT) مانند دستگاه‌های بلیت سلف‌سرویس در ایستگاه‌های راه‌آهن، سینماها و پارکینگ‌ها متصل می‌کنند.

چگونه از کلاه‌برداری کارت‌های تقلبی در امان بمانیم؟

• همیشه با پوشاندن صفحه کلید با دست، کیف یا کیف پول خود، از رمز خود محافظت کنید.
• اگر هنگام استفاده از دستگاه خودپرداز، شخصی در حال تماشای شماست یا هر چیز

مشکوکی را مشاهده کردید، از دستگاه استفاده نکنید و آن را به بانک خود گزارش دهید.
• صورت‌حساب‌های خود را به صورت مرتب بررسی کنید و اگر پرداختی را مشاهده نکردید، فوراً با بانک یا شرکت صادرکننده کارت خود تماس بگیرید.

کلاه‌برداری از طریق کارت گم‌شده و دزدیده‌شده

این کلاه‌برداری زمانی اتفاق می‌افتد که مجرم از یک کارت گم‌شده یا دزدیده‌شده برای خرید یا پرداخت (چه از راه دور یا حضوری) استفاده یا از دستگاه خودپرداز یا شعبه بانک پول خارج کند.
خسارات ناشی از کلاه‌برداری کارت‌های گم‌شده و دزدیده‌شده در سال ۲۰۲۰، ۱۷ درصد کاهش یافت و به ۷۹ میلیون پوند در مقایسه با ۹۵ میلیون پوند سال ۲۰۱۹ رسید. تعداد این کلاه‌برداری‌ها نیز به‌شدت کاهش یافت. اکثر این نوع کلاه‌برداری‌ها با استفاده از کارت‌های به‌دست‌آمده و با وسیله فناوری ساده انجام می‌شود.

چگونه از کلاه‌برداری کارت‌های گم‌شده و دزدیده‌شده در امان بمانیم؟
• همیشه کارت‌های گم‌شده یا دزدیده‌شده را فوراً به بانک یا شرکت کارت خود گزارش دهید.
• صورت‌حساب‌های خود را مرتباً بررسی کنید و اگر پرداختی را مشاهده نکردید، فوراً با بانک یا شرکت کارت خود تماس بگیرید.

کلاه‌برداری از طریق کارت شناسایی

این نوع کلاه‌برداری زمانی اتفاق می‌افتد که مجرم از یک کارت یا مشخصات کارت به‌دست‌آمده، به همراه اطلاعات شخصی دزدیده‌شده برای بازکردن یا تصاحب حساب کارتی به نام شخص دیگری استفاده کند. این نوع کلاه‌برداری به دو دسته تقسیم می شود: کلاه‌برداری از شخص ثالث و کلاه‌برداری دراختیارگرفتن حساب.
خسارات ناشی از سرقت کارت شناسایی در سال ۲۰۲۰ با ۲۱ درصد کاهش به ۲۹٫۷ میلیون پوند رسید و تعداد موارد با کاهش ۳۶ درصدی به ۳۴ هزار و ۵۴۵ مورد رسید. اطلاعات نشان می‌دهد که محرک اصلی سرقت شناسه کارت، جمع‌آوری داده‌ها توسط مجرمان از طریق روش‌هایی از جمله ایمیل‌های فیشینگ، متن‌های کلاه‌برداری و سرقت نامه از صندوق‌های پستی خارجی و ساختمان‌های مسکونی است.

چگونه از کلاه‌برداری کارت شناسایی در امان بمانیم؟
• هنگام نقل مکان به خانه جدید، به بانک، شرکت صادرکننده کارت و سایر سازمان‌ها

آدرس جدید خود را اطلاع دهید.
• اسناد ناخواسته از جمله صورت‌حساب‌ها، صورت‌حساب‌های بانکی یا پست‌هایی را که به نام شما هستند، ترجیحاً از بین ببرید.
• نسخه‌های گزارش اعتبار شخصی خود را به طور منظم از یک آژانس مرجع اعتبار درخواست کنید تا هر ورودی را که نمی‌شناسید، بررسی کنید.
• تا حد امکان اطلاعات شخصی کمتری درمورد خود در رسانه‌های اجتماعی ارائه دهید و فقط دعوت‌های افرادی را که می شناسید، بپذیرید.
• می‌توانید برای حضور در سرویس ثبت حفاظتی Cifas با پرداخت هزینه‌ای که پرچمی را در کنار نام و مشخصات شخصی شما در پایگاه داده‌های ملی امن قرار می‌دهد، درخواست دهید.
• شرکت‌ها و سازمان‌هایی که به عنوان اعضای پایگاه داده‌ها ثبت‌نام کرده‌اند، می‌توانند ببینند که شما در معرض خطر هستید و اقدامات بیشتری برای محافظت از شما انجام دهند و از استفاده مجرمان از اطلاعات شما برای درخواست محصولات یا خدمات جلوگیری کنند.
• مراقب باشید اگر افراد دیگر به صندوق پستی شما دسترسی دارند. اگر فکر می‌کنید صندوق پستی شما دزدیده شده با اداره پست تماس بگیرید.
• هر گونه کارت اعتباری یا نقدی گم‌شده یا دزدیده‌شده را فوراً فاقد اعتبار کنید.
• هنگام استفاده از کارت خود از طریق تلفن، اینترنت یا در مغازه‌ها اطلاعات شخصی خود را با اطمینان از اینکه دیگران نمی‌توانند شما را بشنوند یا اطلاعات شما را ببینند، ایمن نگه دارید.
• اگر پاسپورت، گواهی‌نامه رانندگی، کارت یا سایر اطلاعات شخصی شما مفقود شده یا به سرقت رفته، فوراً با سازمانی که آن را صادر کرده تماس بگیرید.

کلاه‌برداری از کارت‌هایی که به دست گیرنده نرسیده است

این نوع کلاه‌برداری زمانی اتفاق می‌افتد که کارتی در حین حمل‌ونقل، پس از ارسال کارت توسط صادرکننده و قبل از دریافت کارت توسط گیرنده واقعی، به سرقت می‌رود.

چگونه از این نوع کلاه‌برداری در امان بمانیم؟

• اگر منتظر کارت جدیدی هستید و هنوز به دست شما نرسیده، برای کسب اطلاع، با بانک یا شرکت صادرکننده کارت خود تماس بگیرید.
• در صورت نقل مکان به خانه جدید، فوراً به بانک یا شرکت کارت خود اطلاع دهید. از سرویس تغییر مسیر پست برای حداقل یک سال استفاده کنید.

• اگر در ملکی زندگی می‌کنید که ممکن است افراد دیگر به نامه‌های شما دسترسی داشته باشند، مانند یک آپارتمان، بیشتر مراقب باشید. در برخی موارد، بانک یا شرکت صادرکننده کارت شما می‌تواند این کار را برای شما ترتیب دهد.

ضررهای ناشی از کلاه‌برداری کارت دریافت‌نشده، در سال ۲۰۲۰ با ۱۵ درصد کاهش به ۴٫۴ میلیون پوند رسید. با این حال، حجم پرونده‌ها هفت درصد افزایش یافت. مجرمان معمولاً دارایی‌ها را با صندوق‌های پستی مشترک، مانند آپارتمان‌ها، سالن‌های دانشجویی و صندوق‌های پست خارجی هدف قرار می‌دهند تا این نوع کلاه‌برداری را انجام دهند.

کلاه‌برداری از کارت‌های خرده‌فروشی در خرید حضوری

کلاه‌برداری کارت خرده‌فروشی در بریتانیا تمام تراکنش‌هایی را که شخصاً در یک فروشگاه در بریتانیا انجام می‌شود، پوشش می‌دهد. ضررهای ناشی از تقلب در خریدهای حضوری در خیابان‌های بریتانیا با ۲۴ درصد کاهش در سال ۲۰۲۰ به ۴۸٫۹ میلیون پوند رسید. با توجه به دوره‌های طولانی در سال ۲۰۲۰ که اکثر مغازه‌ها به دلیل محدودیت‌های کووید-۱۹ بسته شدند، به طور شگفت‌انگیزی موارد این نوع کلاه‌برداری کاهش یافت. اکثر این کلاه‌برداری‌ها با استفاده از تکنیک‌های ساده فناوری انجام می‌شود و کلاه‌برداران راه‌هایی برای سرقت کارت و رمز آن برای انجام تراکنش‌های جعلی در مغازه‌ها پیدا می‌کنند. مجرمان همچنین از روش‌های مختلف مهندسی اجتماعی برای فریب قربانیان استفاده می‌کنند تا کارت‌های خود را در جلوی خانه‌شان تحویل دهند که اغلب به عنوان کلاه‌برداری پیک شناخته می‌شود.

این دسته شامل آن کلاه‌برداری‌هایی است که شامل عملکرد بدون تماس در کارت‌های پرداخت و دستگاه‌های تلفن همراه می‌شود. کلاه‌برداری بدون تماس در کارت‌های پرداخت و دستگاه‌ها همچنان کم است.

کلاه‌برداری اینترنتی / تجارت الکترونیک

در سال ۲۰۲۰ حدود ۳۷۶ میلیون پوند تقلب در تجارت الکترونیک روی کارت‌ها انجام شد که ۶۶ درصد از کل کلاه‌برداری‌های کارت‌های بانکی و ۸۳ درصد از کل کلاه‌برداری‌های خرید از راه دور را شامل می‌شود. به‌خطرافتادن داده‌ها، از جمله از طریق هک داده‌ها در اشخاص ثالث مانند خرده‌فروشان، عامل اصلی این نوع کلاه‌برداری است.

کلاه‌برداری از کارت‌های بانکی در دستگاه‌های پرداخت نقدی بریتانیا

این ارقام شامل تراکنش‌های متقلبانه‌ای است که در ماشین‌های پرداخت پول نقد در بریتانیا انجام می‌شود، یا با استفاده از کارت سرقت‌شده یا در جایی که حساب کارت

بانکی توسط مجرم در اختیار قرار گرفته است. در همه موارد، کلاه‌بردار باید به رمز و کارت اصلی دسترسی داشته باشد. برخی از این کلاه‌برداری‌های ناشی از نگه‌داشتن رمز توسط دارندگان کارت در کیف پول، توسط سارق دزدیده و بعد از حساب کارت برداشت می‌شود. به‌خطرافتادن یا سرقت کارت به سه روش اصلی انجام می‌شود:

دستگاه های به‌دام‌انداختن کارت: این دستگاه‌ها در داخل شیار کارت در دستگاه پول نقد قرار می‌گیرند و از بازگرداندن کارت به دارنده کارت جلوگیری می‌کنند. برای گرفتن رمز کارت، مجرم از دوربین کوچکی که به دستگاه متصل است استفاده می‌کند، یا اینکه واردکردن رمز را توسط دارنده کارت مشاهده می‌کند. هنگامی که مشتری دستگاه را ترک می‌کند، مجرم دستگاه و کارت را خارج و متعاقباً از آن برای برداشت پول نقد استفاده می‌کند.

دستگاه‌های اسکیمینگ: این دستگاه‌ها برای ضبط جزئیات از نوار مغناطیسی استفاده می‌کنند. در حالی که یک دوربین مینیاتوری مرز وارد شده را ضبط می‌کند، یک کارت نوار مغناطیسی جعلی تولید و از رمز اصلی برای برداشت پول نقد استفاده می‌شود.

مشاهده‌ای عینی: تکنیک دیگری که مجرمان برای به‌دست‌آوردن رمز استفاده می‌کنند مشاهده عینی از روی شانه فرد دارنده کارت است. سپس مجرم با پرت‌کردن حواس دارنده کارت، اقدام به جیب‌بری کرده و کارت را سرقت می‌کند.

کلاه‌برداری از کارت‌ها در خارج از کشور

این دسته کلاه‌برداری‌هایی را پوشش می‌دهد که در خارج از کشور در کارت‌های صادرشده در بریتانیا رخ می‌دهد. اکثر (۸۶ درصد) این نوع کلاه‌برداری‌ها به تقلب خرید از راه دور در خرده‌فروشان خارج از کشور نسبت داده می‌شود. این دسته همچنین شامل مواردی می‌شود که مجرمان، جزئیات نوار مغناطیسی را از کارت‌های صادرشده در بریتانیا می‌دزدند تا کارت‌های تقلبی بسازند و در کشورهایی که هنوز کارت‌ها دارای تراشه و رمز نیستند، استفاده شوند. زیان این نوع کلاه‌برداری برای سال ۲۰۲۰، ۱۵۹٫۷ میلیون پوند بود که در مقایسه با سال ۲۰۰۸ که ۲۳۰٫۱ میلیون پوند بود، ۳۱ درصد کاهش داشت.

کلاه‌برداری از چک

زیان ناشی از کلاه‌برداری چک به ۱۲٫۳ میلیون پوند در سال ۲۰۲۰ کاهش یافت. این زیان در سال قبل از آن ۵۳٫۶ میلیون پوند بود. در همین حال حجم چک‌های جعلی ۵۶ درصد کاهش یافت. کاهش تقلب در چک احتمالاً ناشی از کاهش مداوم استفاده از چک است که به نوبه خود با تأثیر محدودیت‌های قرنطینه تشدید شده است.

البته صنعت بانکداری به نظارت‌های داخلی برای مقابله با کلاه‌برداری چک، از طریق

افزودن ویژگی‌های امنیتی پیشرفته در چک‌های تجاری برای شناسایی چک‌های تقلبی در حین انجام فرایند تسویه ادامه می‌دهد.
همچنین نظام بانکی انگلیس به همکاری نزدیک با نهادهای قانونی برای هدف قراردادن باندهای جنایتکاران سازمان‌یافته که کلاه‌برداری از چک را انجام می‌دهند، ادامه می‌دهد.
این همکاری شامل انجام پژوهش‌های بزرگ و مشترک توسط واحد جرایم پرداخت اختصاصی کارت‌های بانکی و پرداخت پول روی یک شبکه کلاه‌برداری چک در سراسر بریتانیا شد که از کسب‌وکارها و موسسات خیریه ۷۵۰ هزار پوند کلاه‌برداری کرده بود.
در مجموع ۲۳۸٫۵ میلیون پوند از کلاه‌برداری چک در سال ۲۰۲۰ جلوگیری شد که ۵۷ درصد کمتر از سال ۲۰۱۹ است. این نشان‌دهنده این واقعیت است که سطح کلاه‌برداری در سال ۲۰۲۰ کاهش یافته است.

سه نوع کلاه‌برداری چک وجود دارد:

- دستکاری در رقم و نام چک
- چک‌های تقلبی
- چک با امضای جعلی

چگونه از تقلب در چک در امان بمانیم؟

• همیشه چک‌ها را با استفاده از خودکاری که جوهر پاک‌نشدنی دارد صادر کنید.
• در تمام فضاهای استفاده‌نشده، از جمله بعد از نام گیرنده، یک خط بکشید.
• دسته‌چک خود را در مکانی امن نگه دارید و برگه چک‌های مفقودشده را فوراً به بانک خود گزارش دهید.
• صورت‌های خود را به طور منظم بررسی کنید و اگر پرداختی را مشاهده نکردید، فوراً با بانک خود تماس بگیرید.

کلاه‌برداری غیرمجاز بانکی از راه دور

خسارات ناشی از کلاه‌برداری بانکی از راه دور به سه دسته بانکداری اینترنتی، بانکداری تلفنی و بانکداری تلفن همراه دسته‌بندی می‌شوند. این کلاه‌برداری زمانی اتفاق می‌افتد که مجرمی از طریق یکی از این سه کانال بانکی از راه دور، به حساب بانکی یک فرد دسترسی پیدا کند و پولی را به صورت غیرمجاز از حساب منتقل کند.
کل کلاه‌برداری بانکی از راه دور در سال ۲۰۲۰ به ۱۹۷٫۳ میلیون پوند رسید که ۳۱ درصد بیشتر از سال ۲۰۱۹ بود. تعداد موارد کلاه‌برداری بانکی از راه دور با ۶۸ درصد افزایش به ۷۳ هزار و ۶۴۰ مورد رسید. این نشان‌دهنده تعداد بیشتری از افرادی است که اکنون به طور منظم

از اینترنت، تلفن و بانکداری تلفن همراه استفاده می‌کنند. تلاش کلاه‌برداران برای سوء استفاده از این امر نیز به تبع این استفاده زیاد افزایش یافته است. در سال ۸۱،۲۰۱۹ درصد از جمعیت بزرگسال حداقل از یک نوع بانکداری از راه دور استفاده می‌کردند. علاوه بر این، پاندمی کرونا و محدودیت‌های تردد و افزایش افرادی که دورکاری می‌کنند، باعث شد تعداد فزاینده‌ای از مردم به سمت بانکداری آنلاین و موبایل بانک سوق داده شوند و این مسئله زمینه را برای فعالیت بیشتر کلاه‌برداران در این حوزه فراهم کرد.

در مجموع ۳۹۳٫۸ میلیون پوند تلاش برای کلاه‌برداری بانکی از راه دور توسط سیستم‌های امنیتی بانک در طول سال ۲۰۲۰ متوقف شد. این معادل دو پوند از هر سه پوند تلاش برای کلاه‌برداری است. علاوه بر این، ۱۵ درصد (۳۰٫۲ میلیون پوند) از زیان تمام کانال‌های بانکی از راه دور پس از این حادثه جبران شد.

نظام بانکی انگلیس به طرق زیر، در حال مقابله با کلاه‌برداری بانکی از راه دور است:

- سرمایه‌گذاری مستمر در توسعه سیستم‌های امنیتی پیشرفته، از جمله روش‌های پیچیده احراز هویت مشتریان، مانند استفاده از بیومتریک و تجزیه‌وتحلیل رفتار مشتری.
- گسترش طرح پروتکل بانکی؛ طرحی که به کارکنان شعب بانک اجازه می‌دهد زمانی که فکر می‌کنند از مشتری کلاه‌برداری شده، به پلیس هشدار دهند.
- سرمایه‌گذاری در کمپین Take Five to Stop Fraud برای آموزش مشتریان درمورد اینکه چگونه می‌توانند از خود در برابر کلاه‌برداری محافظت کنند.
- به‌اشتراک‌گذاری اطلاعات درمورد این نوع کلاه‌برداری به طوری که سیستم‌های امنیتی بتوانند برای جلوگیری از آخرین تهدیدات سازگار شوند.
- همکاری با مجریان قانون، دولت، صنعت مخابرات و سایرین برای بهبود بیشتر امنیت، شناسایی و محاکمه مجرمان.

کلاه‌برداری در بانکداری اینترنتی

به طور معمول، مجرمان از طیف وسیعی از تکنیک‌های مهندسی اجتماعی استفاده می‌کنند تا قربانیان را فریب دهند تا آنها اطلاعات شخصی و مالی خود مانند رمزهای یک بار مصرف بانکداری اینترنتی و جزئیات ورود را ارائه دهند. این تکنیک‌ها شامل استفاده از حجم بالایی از تماس‌های کلاه‌برداران برای جعل هویت، ارسال ایمیل‌ها یا پیام‌های متنی به قربانیان با هدف سوءاستفاده از شرایط پاندمی و جعل هویت سازمان‌های مورد اعتماد مانند وزارت بهداشت و بیمارستان‌ها، ارائه‌دهندگان خدمات اینترنتی و شرکت‌های تجارت الکترونیک است. سپس کلاه‌برداران از جزئیات دزدیده‌شده برای دسترسی به حساب آنلاین مشتری و انجام یک تراکنش غیرمجاز استفاده می‌کنند.

این واقعیت که بسیاری از مردم از خانه کار می‌کنند، به این معناست که آنها زمان بیشتری

را به صورت آنلاین سپری می‌کنند و خرید اینترنتی بیشتری انجام می‌دهند، بنابراین بیشتر مستعد هستند در معرض این نوع کلاه‌برداری‌ها قرار بگیرند. اطلاعات نشان می‌دهد که مشتریان در تمام گروه های سنی قربانی این کلاه‌برداری‌ها می‌شوند، اما گروه‌های سنی جوان‌تر بیشترین تعداد قربانیان هستند.

در همین حال، بیش از دو سوم بزرگسالان بریتانیا (۷۲ درصد) در سال ۲۰۱۹ از بانکداری آنلاین استفاده کردند و این میزان در سال ۲۰۲۰ در نتیجه پاندمی افزایش یافته است. با افزایش استفاده از اینترنت و بانکداری آنلاین، تلاش مجرمان برای سرقت پول از طریق این کانال‌ها نیز افزایش می‌یابد. مجرمان معمولاً ادعا می‌کنند که از یک طرف با یک سرویس فناوری اطلاعات یا ارائه‌دهنده خدمات اینترنتی تماس می‌گیرند و مشتریان را متقاعد می‌کنند برنامه‌های دسترسی از راه دور را روی رایانه شخصی یا دستگاه‌های لپ‌تاپ خود دانلود و نصب کنند.

افزایش قابل توجهی در استفاده از وب‌سایت‌های فیشینگ برای به‌دست‌آوردن اعتبار بانکی آنلاین مشتریان مشاهده شده است. بیش از ۲۵ هزار وب‌سایت فیشینگ با لوگوی بانکی در سال ۲۰۲۰ شناسایی و حذف شدند که چهار برابر بیشتر از سال ۲۰۱۹ بوده است.

در مجموع ۳۲۶٫۲ میلیون پوند تلاش برای کلاه‌برداری بانکداری اینترنتی توسط سیستم‌های امنیت بانکی انگلیس در سال ۲۰۲۰ متوقف شد. این معادل ۶٫۷۱ پوند از هر ۱۰ پوند تلاش برای جلوگیری از کلاه‌برداری است. علاوه بر این، ۱۶ درصد (۲۵٫۳ میلیون پوند) از زیان‌های کانال بانکداری اینترنتی پس از این حادثه جبران شد.

چگونه از کلاه‌برداری بانکداری اینترنتی در امان بمانیم؟

• یک بانک یا سازمان واقعی هرگز با شما تماس نخواهد گرفت تا رمز عبور شما را بخواهد. فقط اطلاعات شخصی یا مالی خود را برای استفاده از سرویسی که رضایت خود را اعلام کرده‌اید، مورد اعتماد شماست و انتظار دارید با شما تماس گرفته شود، ارائه دهید.

• در صورت کلاه‌برداری، همیشه رویکردهای عجیب را زیر سوال ببرید و با شرکت تماس بگیرید.

• فریب نخورید و به یک کلاه‌بردار اجازه دسترسی به جزئیات شخصی یا مالی خود را ندهید. هرگز روی لینکی در ایمیل یا متنی عجیب، کلیک نکنید.

• مطمئن شوید که به‌روزترین نرم‌افزار امنیتی از جمله آنتی ویروس را روی رایانه خود نصب کرده‌اید. برخی از بانک‌ها نرم‌افزار امنیتی رایگان ارائه می‌دهند، بنابراین وب‌سایت بانک خود را بررسی کنید.

کلاه‌برداری از تلفن‌بانک

این نوع کلاه‌برداری زمانی اتفاق می‌افتد که مجرم به حساب تلفن‌بانک قربانی دسترسی پیدا کند و پولی را به طور غیرمجاز از آن خارج کند. مشابه کلاه‌برداری در بانکداری اینترنتی، مجرمان اغلب از تاکتیک‌های مهندسی اجتماعی برای فریب مشتریان برای افشای جزئیات امنیتی حساب خود استفاده می‌کنند، سپس برای متقاعدکردن اپراتور تلفن‌بانک مبنی بر اینکه آنها صاحب حساب واقعی هستند، تلاش می‌کنند.

در مجموع ۵۸ میلیون پوند تلاش برای کلاه‌برداری تلفنی بانکی توسط سیستم‌های امنیتی بانک در سال ۲۰۲۰ متوقف شد. این مبلغ معادل ۷٫۸۲ پوند از هر ۱۰ پوند کلاه‌برداری است. علاوه بر این، ۱۲ درصد (۲ میلیون پوند) از زیان‌های کانال بانکی تلفنی پس از این حادثه جبران شد.

کلاه‌برداری از موبایل‌بانک

کلاه‌برداری از تلفن همراه زمانی اتفاق می‌افتد که یک مجرم از جزئیات حساب بانکی به‌خطرافتاده، برای دسترسی به حساب بانکی مشتری از طریق یک برنامه بانکی که فقط در یک دستگاه تلفن همراه دانلود شده، استفاده کند. در سال ۲۰۱۹، حداقل ۵۰ درصد از بزرگسالانی که در بریتانیا زندگی می‌کنند از یک برنامه بانکداری تلفن همراه یا روی تلفن یا رایانه خود استفاده می‌کردند که نسبت به سال ۲۰۱۵، ۳۳ درصد افزایش یافته و این احتمال وجود دارد که با آشنایی بیشتر و راحت‌ترشدن مردم با آن، این میزان افزایش یابد.

در مجموع ۹٫۶ میلیون پوند تلاش برای کلاه‌برداری در بانکداری تلفن همراه توسط سیستم‌های امنیتی بانک در سال ۲۰۲۰ متوقف شد. این مبلغ معادل ۳٫۰۹ پوند از هر ۱۰ پوند تلاش برای جلوگیری از کلاه‌برداری است. علاوه بر این، ۱۳ درصد (۲٫۹ میلیون پوند) از زیان‌های کانال بانکی تلفن همراه پس از این حادثه جبران شد.

چگونه از کلاه‌برداری موبایل‌بانک در امان بمانیم؟

- فریب نخورید و به یک کلاه‌بردار اجازه دسترسی به اطلاعات شخصی یا مالی خود را ندهید. هرگز به طور خودکار روی پیوندهای موجود در ایمیل‌ها یا متن‌های غیرمنتظره کلیک نکنید و همیشه رویکردهای عجیب را زیر سوال ببرید.
- مراقب پیام‌های متنی باشید که شما را تشویق می‌کنند فوراً از یک وب‌سایت دیدن کنید یا با شماره‌ای تماس بگیرید تا جزئیات خود را تائید یا به‌روزرسانی کنید.
- در صورت کلاه‌برداری، همیشه رویکردهای عجیب را زیر سوال ببرید. در عوض، مستقیماً با استفاده از یک ایمیل یا شماره تلفن شناخته‌شده با شرکت یا بانک تماس بگیرید.

داتین

ارائه‌دهنده راهکارهای
بانکی، مالی و بیمه‌ای

www.dotin.ir