جرائم پولشویی در دوران شیوع کرونا

نسرین عرب بافرانی

جرائم مالی در دوران بحران همه گیر ی

پلیس بین‌الملل، افزایش تهدیدات سایبری مرتبط به باج‌افزارها و بدافزارها را طی بیانیه‌ای جهانی به ۱۹۴ کشور عضو اعلام کرده است. در این خصوص اعضای FATF گزارشاتی مبنی بر افزایش پولشویی و تروریسم مالی مرتبط به کووید ۱۹ ارائه کرده‌اند:

۱- افزایش سوءاستفاده از خدمات مالی و دارایی‌های مجازی به‌منظور راه‌هایی برای انتقال و محوکردن پول‌های غیرقانونی

۲- جرائم مربوط به سوءاستفاده از وجوه

دولتی و کمک‌های مالی بین‌المللی به‌منظور تأمین خسارت مشکلات ایجاد شده ناشی از همه‌گیری کووید ۱۹.

در سطح ملی، سازمان‌های اجرای قانون، هشدارهایی در ارتباط با این تهدیدات صادر کرده‌اند. برای مثال مقامات امنیتی در اتحادیهٔ اروپا (EU) و ایالت متحدهٔ آمریکا (US) بیانیهٔ مشترک فوری به‌منظور افزایش سطح امنیت اشخاص و شرکت‌ها نسبت به ایمیل‌ها و پیامک‌هایی که به‌نظر می‌رسد از جانب اشخاص و سازمان‌های معتبر مانند سازمان بهداشت جهانی به‌منظور پیشنهاد راه‌های درمان یا معرفی تجهیزات پزشکی مؤثر برای کووید۱۹ ارسال شود، هشدار داده‌اند. بیانیه همچنین به جرائم سایبری مرتبط به این دوران که از طریق وسائل و تجهیزات کار از راه دور مانند ویدئو کنفرانس‌ها می‌توانند اتفاق افتد اشاره کرده است[1]. سازمان اجرایی قانون، هدف جرائم سایبری در این دوران را به سرقت بردن اطلاعات شخصی افراد مانند نام کاربری و کلمه عبور اشخاص می‌داند، که این موضوع از طریق درخواست دانلود یک سری از نرم‌افزارها که به‌اصطلاح بدافزار نامیده می‌شوند اتفاق می‌افتد.

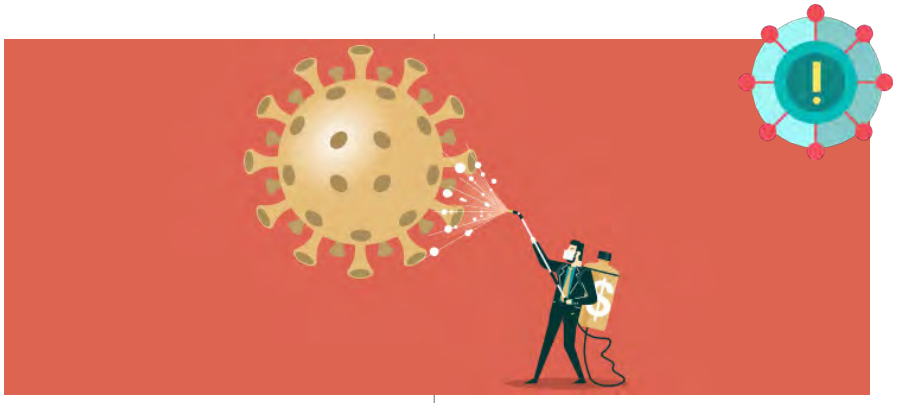
گزارشات، منعکس‌کنندهٔ افزایش جرائم سایبری در دوران همه‌گیری کرونا است؛ به‌عنوان مثال شرکت کربن بلک (Carbon Black) ، که یک شرکت امنیت سایبری است، گزارشاتی مبنی بر افزایش حملات سایبری در مارچ ۲۰۲۰ نسبت به فوریه ۲۰۲۰، به میزان ۱۴۸درصد کرده است که در میان بخش‌های مختلف، صنعت تأمین مالی با ۳۸درصد افزایش حملات سایبری در میان مؤسسات مالی، هدف اصلی حملات سایبری بوده است. به‌طور مشابه مرکز تجزیه و تحلیل و انتشار اطلاعات مالی، بیش از ۱۵۰۰ دامنه با ریسک بالا در زمینه‌های مالی در ۱ ژانویه ۲۰۲۰ یا قبل از آن را که مرتبط به کووید ۱۹ است، شناسایی کرده است. سایت گوگل از ارسال روزانه ۱۸ میلیون ایمیل و نرم‌افزارهای مخرب به‌علاوه روزانه بیش از ۲۴۰ میلیون پیامک مخرب را با محتوای کووید ۱۹ در اوائل اپریل ۲۰۲۰ گزارش داده است.

شرایط موجود، فشار زیادی روی انعطاف‌پذیری سایبری مؤسسات مالی و تأمین‌کنندگان خدمات تکنولوژیکی اشخاص وارد کرده است. در جریان تغییرات پیش آمده، صنعت مالی در مقابله با حملات سایبری رشد زیادی پیدا کرده است و در نتیجه برای مقابله با حملات سایبری همکاری‌های بین المللی افزایش پیدا کرده است. ضمناً نمی‌توان گفت این قبیل سناریوها فقط در شرایط قرنطینهٔ فعلی یا آتی اتّفاق می‌افتد بلکه در هر موقعیتی که عدم امنیت در جامعه باشد وقوع چنین سناریوهایی وجود دارد.

این قبیل جرائم همچنین در نتیجه خلاء و ضعف در سیستم دفاعی ضدپولشویی در مؤسسات مالی در شرایط همه‌گیری ایجاد شده است. همانطور که در بالا ذکر شد مؤسسات مالی در حال حاضر به‌علت فاصله‌گذاری اجتماعی و تعطیلی ادارات با مشکلاتی از قبیل تأیید هویت مشتریان (براساس شناسنامه، کارت ملی، پاسپورت و...) مواجه شده‌اند. همین عامل زمینهٔ بسیار مساعدی را برای پولشویان، به‌ویژه زمانی که مؤسسات مالی به وسائل و امکانات تأیید هویت مشتریان از راه دور مجهز نباشند، فراهم می‌کند. نیاز به منابع مازاد به‌منظور مطمئن شدن از انجام فرایند کار شرکت‌ها به‌طور مؤثر می‌توانند به این مفهوم باشد که مؤسسات مالی نظارت کافی روی تراکنش‌های مشکوک ندارند. مقامات عالی‌رتبه نیز در شرایط ایجاد شدهٔ ناشی از بحران همه‌گیری کرونا مجبور به، به تعویق انداختن فعالیت‌های ضدپولشویی و انجام دیگر فعالیت‌ها و صرفاً نظارت غیرمستقیم بر فعالیت‌های ضدپولشویی هستند. همچنین تعداد زیادی از مراجع قضایی گزارشاتی از افزایش برداشت‌های وجه نقد علی‌رغم محدودیت‌های برداشت وجه نقد، اعلام شده در دوران کرونا به‌منظور مساعد بودن اسکناس جهت اهداف پولشویی ارائه کرده‌اند[2].

- افزایش فعالیت‌های پولشویی:

شیوع بیماری کرونا باعث ایجاد عکس‌العمل‌های مختلف از سوی دولت‌های مختلف شده است و این عکس‌العمل



به میزان گستردگی بیماری در کشورها بستگی دارد و طیف وسیعی از فعالیت‌های اقتصادی و همچنین فعالیت‌های مربوط به معافیت مالیاتی تا محدودیت در سفرها و قرنطینه‌های اجباری را شامل می‌شود. در شرایط همه‌گیری، دغدغهٔ دولت‌ها حفظ سلامتی شهروندانشان است و به بعضی فعالیت‌ها از جمله پولشویی و تروریسم مالی توجه نمی‌شود. ریسک‌های مربوط به این دوران اغلب بر اثر فعالیت‌های زیر ایجاد می‌شود:

- قرنطینه شدن افراد در منازل و انجام کارها از راه دور
- تعطیلی مشاغل غیرضروری و در نهایت روی آوردن مشاغل ضروری و غیرضروری به خدمات آنلاین و مجازی
- به‌علت گستردگی شیوع بیماری و افزایش تقاضا برای خدمات و تجهیزات پزشکی و همچنین برخی داروها، کاهش محسوسی در این قبیل داروها و تجهیزات ایجاد شده است.
- علی‌رغم تعطیلی و غیرحضوری شدن اکثر فعالیت‌های اجتماعی، شرکت‌ها و مؤسسات مالی و بانک‌ها و بیمه همچنان به فعالیت حضوری ادامه دادند
- تعطیلی شرکت‌ها به‌علت قرنطینهٔ عمومی باعث بیکاری اکثر کارمندان و کاهش درآمد دولت‌ها و رکود اقتصادی شده است که این عوامل بر رفتار اشخاص و شرکت‌ها تأثیرگذار است.
- برنامهٔ کاری فعالیت‌های دولت‌ها تغییر کرده است و یکسری فعالیت‌های جدید در الویت کار قرار گرفته‌اند.
- حجم معاملات و همچنین مسافرت‌ها به‌منظور جلوگیری از انتقال ویروس کاهش پیدا کرده است و در مقابل فعالیت‌های جنایی و درآمد حاصل از آنها افزایش پیدا کرد.

– **افزایش تقلب:**

مشاهدات و گزارشات اعضای FATF حاکی از افزایش فعالیت‌های متقلّبانه در دوران شیوع بیماری کرونا است که اهمّ این فعالیت‌ها شامل:

- **سوءاستفاده از نام، صدا و هویت اشخاص و مقامات عالی‌رتبه:** در شرایط به‌وجود آمدهٔ ناشی از شیوع ویروس کرونا بسیاری از مجرمان به شیوه‌های مختلف از جمله استفاده از تلفن و ایمیل و معرفی کردن خود به‌عنوان مقامات عالی‌رتبه و درخواست دریافت پول و مشخصات حساب‌های بانکی با افراد و شرکت‌ها تماس برقرار کرده‌اند. در بعضی موارد آنها درخواست دریافت کمک به‌منظور تأمین خدمات پزشکی برای درمان مثلاً فلان مقام عالی‌رتبه در ازای اعطای بخشودگی مالیاتی برای شخص کمک کننده را کرده‌اند[3].
- **جعل کردن اقلام اساسی (مانند داروها و تجهیزات پزشکی):** شیوع گستردهٔ بیماری کرونا باعث افزایش تقاضا برای یکسری خدمات و تجهیزات پزشکی و درمانی و داروهای خاص شده است و این عامل باعث افزایش درآمدهای غیرقانونی آنلاین شده است. در این شرایط کلاهبرداران خود را کارمندان شرکت‌ها یا مؤسسات خیریهٔ تأمین‌کنندهٔ ماسک، تجهیزات درمانی و کیت‌های تشخیص کرونا معرفی و درخواست دریافت اطلاعات کارت اعتباری مشتریان را می‌کنند در حالی که این کالاها یا هرگز به مشتریان تحویل داده نمی‌شود یا کالاهای جعلی و تقلبی تحویل داده می‌شود[4]. ضمناً در بعضی موارد مشاهده شده است که مشتری وجه کالا و خدمات را پرداخت کرده است و پس از ماه‌ها انتظار و پیگیری‌های مداوم، کالا را در مکانی غیراز مکان ثبت شده در فرم درخواست کالا دریافت کرده است (گزارش توسط پلیس سنگاپور[5]). اعضای FATF همچنین گزارشاتی مبنی بر ارائهٔ راه‌های درمان تقلبی و غیراصلی به مشتریان و همچنین بازاریابی و فروش محصولات غیرقانونی تحت عنوان درمان‌های معجزه‌آسا را داده‌اند[6].
- **جمع‌آوری پول برای خیریه‌های تقلبی:** اعضای FATF همچنین از جمع‌آوری پول برای مقاصد خیرخواهانه برای خیریه‌های تقلبی (خیریه‌هایی که ماهیت قانونی ندارند) گزارش داده‌اند. در اینگونه موارد کلاهبرداران با معرفی خود تحت عنوان مؤسسات خیریه یا سازمان‌های بین‌المللی دریافت‌کنندهٔ کمک‌های مردمی از طریق ایمیل و به‌منظور رفع مشکلات ناشی از کووید ۱۹ سعی در

جمع‌آوری پول و کمک‌های مالی از افراد و شرکت‌ها کرده‌اند و درخواست دریافت اطلاعات کارت بانکی آنها را کرده‌اند یا از طریق کیف پول‌های تقلبی دیجیتالی سعی در به‌دست آوردن پول آنها کرده‌اند.

■ **تحصیل پول از طریق فعالیت‌های سرمایه‌گذاری متقلّبانه:** یکی از مشکلات اقتصادی به‌وجود آمده بر اثر شیوع کرونا افزایش تحصیل پول از طریق سرمایه‌گذاری‌های تقلبی است. به این ترتیب که کلاهبرداران خود را به‌عنوان تولید کنندهٔ محصولاتی معرفی می‌کنند که محصولاتشان در مقایسه با محصولات مشابه، در شناسایی و جلوگیری و درمان کووید ۱۹ بسیار مؤثرتر است[۷]. همچنین اعضای FATF از فعالیت کلاهبرداران در زمینهٔ ارزش‌گذاری سهام شرکت‌ها گزارش داده‌اند. به‌عنوان مثال سهام شرکت microcap که اغلب توسط شرکت‌های کوچک عرضه می‌شود، توسط فعالیت‌های کلاهبرداران دستخوش آسیب شده است. بدین صورت که کلاهبرداران با تشکیل صف‌های خرید ساختگی و در نتیجه افزایش تقاضای خرید سهام این شرکت، قیمت سهام را بالا برده‌اند درحالی‌که تعداد سهام این شرکت محدود و قیمت واقعی آن پایین است و همین عامل باعث انتشار اطلاعات مالی اشتباه راجع به شرکت‌ها می‌شود[۸] (گزارش سازمان بورس اوراق بهادار ایالت متحده)

- جرائم سایبری

پس از شیوع همه‌گیری کووید ۱۹ افزایش بسیار بالایی در سطح حملات سایبری اتفاق افتاد، که عمدتاً از طریق ایمیل‌های تقلبی و پیام‌های تلفن همراه که عمدتاً از طریق کمپین‌های تقلبی و دروغین منتشر می‌شده است. این حملات عمدتاً از طریق لینک‌های وب‌سایت به همراه ضمائم مخرب و دروغین است و هدف تمام آنها به‌دست آوردن اطلاعات مربوط به حساب‌های بانکی افراد است. جرائم سایبری عمدتاً به روش‌های زیر ایجاد می‌شود:

■ **از طریق پیام‌های کوتاه و ایمیل‌های تقلبی:** کلاهبرداران با وارد کردن بدافزارها به کامپیوترهای شخصی و موبایل‌ها شروع به بهره‌برداری از شرایط به‌وجود آمده بر اثر کووید ۱۹ هستند. به‌عنوان مثال، کلاهبرداران سایبری خود را به‌عنوان نمایندهٔ سازمان بهداشت جهانی معرفی می‌کنند و با ارسال پیام کوتاه یا ایمیل‌های حاوی لینک‌های مخرب برای افراد پس از باز کردن لینک‌ها، اطلاعات مربوط به کلمهٔ عبور و نام کاربری حساب بانکی اشخاص مشخص می‌شود (گزارش سازمان بهداشت جهانی[۹])

■ **تحصیل پول از طریق ایمیل‌های شرکتی:** به‌دنبال شیوع گستردهٔ ویروس کرونا و تلاش دولت‌ها برای حفظ سلامت مردم کشورشان، اکثر کارها به‌صورت دورکاری و در منازل از طریق آنلاین انجام می‌شود و به همین میزان کلاهبرداران سایبری با استفاده از ضعف شبکهٔ امنیتی شرکت‌ها به اطلاعات تماس مشتریان و نیز اطلاعات معاملات شرکت‌ها دسترسی پیدا می‌کنند. کلاهبرداران از این اطلاعات استفاده می‌کنند و شرکت‌ها را تهدید به افشای اطلاعات آنها می‌کنند و در نهایت درخواست دریافت وجه را برای واگذار کردن این اطلاعات و واریز آن به حساب‌های غیرقانونی می‌کنند[۱۰]. (گزارش بانک جهانی پول) به‌عنوان مثال دیگر، دریافت ایمیل‌هایی که گویا یکی از شرکای شرکت ارسال شده است و درخواست واریز مبلغ بالایی وجه نقد برای خرید ماسک و وسائل ضدعفونی‌کنندهٔ دست، به حساب مشخصی را کرده باشد.

■ **حملات باج‌افزارها:** گزارش‌ها حاکی از اینست که کلاهبرداران سایبری در حال وارد کردن باج‌افزارها (نرم‌افزارهای پولی) به موبایل‌ها و کامپیوترهای شخصی هستند. به‌عنوان مثال بعضی از اعضای FATF گزارش کرده‌اند کلاهبرداران سایبری با وارد کردن وب‌سایت‌ها و اپلیکیشن‌های مخرب به موبایل یا کامپیوترهای شخصی، با این مضمون که این سایت‌ها و اپلیکیشن‌ها اطلاعات مربوط به کووید ۱۹ را گزارش می‌دهند، غافل از اینکه پس از اجرای این اپلیکیشن‌ها و وب‌سایت‌ها دستگاه شخص قفل می‌شود و برای راه‌اندازی مجدّد از شخص وجه را دریافت می‌کند

و تا پرداخت نکردن وجه، دستگاه مورد نظر از حالت قفل خارج نمی‌شود. ضمناً بعضی از سازمان‌ها بیشتر از دیگر سازمان‌ها در معرض اینگونه حملات قرار می‌گیرند از جمله بیمارستان‌ها و مؤسسات درمانی[11](گزارش اینترپل)

تأثیر روی دیگر جرائم

■ **قاچاق انسان و استثمار کارگران:** شیوع گستردهٔ بیماری کرونا و تعطیلی اکثر بنگاه‌ها و مشاغل باعث کاهش رونق اقتصادی، افزایش نرخ بیکاری و عدم امنیت مالی شده است که می‌توان گفت تمامی این عوامل از جمله فاکتورهایی هستند که می‌توانند زمینه را برای قاچاق انسان و استثمار کارگران محیا کنند. اعضای FATF در حال گزارش به شرکت‌ها در جهت بالا بردن سطح هوشیاری نسبت به استثمار کارگران و قاچاق افراد آسیب‌پذیر هستند[12].

■ **استثمار آنلاین کودکان:** گزارش‌ها حاکی از افزایش تولید و توزیع بازی‌های آنلاین به‌منظور سود بردن از کودکان است. به‌علت تعطیلی مدارس و استفادهٔ بیشتر از بازی‌های آنلاین در دوران قرنطینه، زمینه برای استثمار کودکان فراهم شده است. (گزارش بانک بین‌الملل)

– تغییر رفتارهای مالی

گزارش‌ها حاکی از تغییراتی در رفتار و الگوهای مالی است. بسیاری از بانک‌ها و شعب آنها به‌علت رعایت مسائل بهداشتی و قرنطینه ناشی از کرونا تعطیل شده‌اند و همین موضوع باعث انجام کارها از طریق دورکاری شده است. رکود اقتصادی به‌وجود آمده ناشی از این شرایط باعث ایجاد تغییراتی در وضعیت مالی افراد شده است و منجر به کشف راه‌هایی جهت تأمین مالی‌های خارج از شرایط نرمال و عادی شده است. نمونه‌هایی از این شرایط شامل:

■ **افزایش انجام تراکنش‌ها از راه دور:** به‌علت شیوع گستردهٔ ویروس کرونا، بسیاری از بانک‌ها و شعبات آنها تعطیل شده است و انجام خدمات مشتریان به‌صورت برخط و آنلاین انجام می‌شود. اعضای FATF و FSRB از مجهز نبودن بسیاری از بانک‌ها به ابزارهای تأیید هویت اشخاص (مانند شناسنامه، کارت ملی، پاسپورت و...) از راه دور گزارش داده‌اند لذا در روش برخط تأیید هویت مشتریان برای انجام خدمات به‌تعویق می‌افتد.

■ **عدم آشنائی اکثر افراد به استفاده از روش‌های آنلاین:** بسیاری از اقشار جمعیت مانند افراد پیر و سالخورده، افراد بی‌سواد، گروه‌هایی با سطح درآمد پائین یا در نقاطی که دسترسی به اینترنت در آنجا بسیار محدود است یا اصلاً وجود ندارد ممکن است با نحوهٔ استفاده خدمات آنلاین آشنایی نداشته باشند یا آشنایی کمی داشته باشند در نتیجه این قبیل افراد بیشتر از سایرین ممکن است در معرض خطر افراد سودجو و کلاهبردار قرار بگیرند.

■ **خدمات بانکی غیرمداوم:** به‌علت شرایط رکود اقتصادی بلندمدت ایجاد شده ناشی از شیوع کرونا اعضای FATF و FSRB گزارش کرده‌اند که افراد با مشکلات اقتصادی به دنبال روش‌های غیرتجاری و نامعتبر برای به‌دست آوردن پول هستند که این قبیل افراد ممکن است بیشتر در معرض خطر وعده‌های دروغین افراد کلاهبردار قرار گیرند.

– افزایش بی‌ثباتی مالی

به‌علت همه‌گیری شیوع کرونا در کل دنیا بی‌ثباتی مالی و اقتصادی ایجاد شده است و در این شرایط روش‌های فعالیت کلاهبرداران تغییر کرده است که شامل:

– بدتر شدن وضعیت اقتصادی: در شرایط بد اقتصادی به‌وجود آمده ناشی از کووید ۱۹ کلاهبرداران در حال سرمایه‌گذاری روی ملک و شرکت‌های تجهیزات پزشکی برای به‌دست آوردن پول و در نتیجه پوشاندن پول‌هایی که بر اثر فعالیت‌های غیرقانونی به‌دست آورده‌اند هستند. گروهی از کلاهبرداران وجوه غیرقانونی را از طریق اعطای وام وارد سیستم مالی می‌کنند. ضمناً در برخی موارد کلاهبرداران با اعلام ورشکستگی شرکت‌ها و وارد کردن پول‌های به‌دست آمده از راه‌های غیرقانونی و به بهانهٔ نجات این قبیل شرکت‌ها از وضعیت

ورشکستگی، درواقع پوششی قانونی بر روی وجوه غیرقانونی می‌گذارند.

- **افزایش تراکنش‌های وجه نقد به‌صورت اسکناس:** اعضای FATF به تازگی گزارش کرده‌اند که حجم بالایی وجه نقد به‌صورت الکترونیکی در اوراق بهادار وارد شده است که این موضوع در نتیجه نقدینگی بالای افراد است. اعضای FATF و FSRB همچنین گزارش کرده‌اند با وجود محدودیت در استفاده از اسکناس به‌علت افزایش انتقال ویروس کرونا، حجم بالای وجه نقد از حساب‌های بانکی اشخاص برداشت شده است. افزایش برداشت اسکناس به دلائل زیر می‌تواند منجر به پولشویی و تروریسم مالی شود:

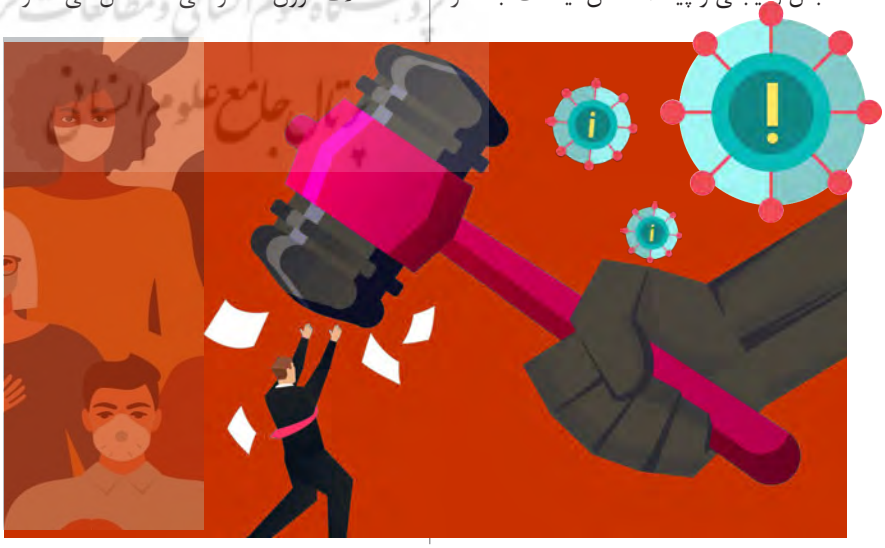
- در شرایط ثبات مالی اکثر افراد به سپرده‌گذاری در بانک روی می‌آورند که این موضوع پوشش مناسبی را برای پولشویی وجوه حاصل از فعالیت‌های غیرقانونی بالاخص به‌صورت اسکناس را فراهم می‌کند.
- اسکناس برای خرید دارایی‌هایی که ارزش بالایی دارند که این ارزش هم در طول زمان باقی می‌ماند و هم می‌تواند در طول دوران رکود اقتصادی مشمول افزایش ارزش افزوده شود و هم به‌راحتی قابل ردیابی و پیدا شدن نیست، به‌کار رود مانند طلا
- افزایش خطر برداشت از حساب بانکی مشتریان از طریق به‌دست آوردن اطلاعات حساب آنها و برداشت وجه نقد به‌صورت اسکناس از دستگاه‌های خودپرداز

- **دارایی‌های مجازی:**

اعضای FATF و FSRB از افزایش خطرات دارایی‌های مجازی گزارش داده‌اند. در یک مورد که اخیراً توسط ادارهٔ دادگستری ایالت متحده گزارش شده است، فردی وجوه حاصل از فروش داروهای تقلبی مربوط به کووید ۱۹ را جهت معاملهٔ دارایی‌های دیجیتالی مانند سهام استفاده کرده است[۱۳].

- **معاملات درون سازمانی[۱۴]:**

گزارش‌ها حاکی از افزایش سرمایه‌گذاری‌های تقلبی به‌علت بی‌ثباتی مالی ناشی از شیوع کووید ۱۹ هستند. تأمین‌کنندگان خدمات مالی در حال نقد کردن و خارج کردن دارایی‌های خود از بازار سهام در پاسخ به عدم اطمینان از شرایط ایجاد شده به‌علت شیوع کووید ۱۹ هستند. سپس این حجم بالای نقدینگی به سمت بازارهای با بازده بالا مانند معاملات درون سازمانی منتقل می‌شود.



اعضای FATF همچنین گزارش‌هایی مبنی بر پیشنهاد افزایش سرمایهٔ شرکت‌هایی که محصولات و داروهای تقلبی تولید می‌کنند، ارائه کرده‌اند.

- **تروریسم مالی**

گزارشاتی مبنی بر هشدارهای ایالت متحده به دولت‌ها درحالی‌که دولت‌ها تمام توجهشان را معطوف به برطرف کردن مشکلات ایجاد شدهٔ ناشی از کووید ۱۹ کرده‌اند فعالیت تأمین مالی گروه‌های تروریستی در حال افزایش است[۱۵]. به موازات افزایش کمک‌های بشردوستانه بین‌المللی در ارتباط با کووید ۱۹، دولت‌ها بایستی روش‌های مبتنی بر ریسک، جهت حذف به خطر افتادن این وجوه از استفاده شدن به‌منظور تأمین نیازهای مالی گروه‌های تروریسم به‌کار گیرند[۱۶].

معیار انعطاف‌پذیری سایبری

در پاسخ به شرایط فعلی ایجاد شده به‌علت شیوع کووید ۱۹ و ظهور حملات سایبری مرتبط به این دوران، پلیس اینترپل راهنمایی‌های بین‌المللی ارائه کرده است. در همین راستا سازمان ملی مسئول امنیت سایبری راهنمایی‌ها و پیشنهادات لازم را اعلام کرده است. به‌عنوان مثال بیانیهٔ مشترک سازمان امنیت سایبری اتحادیه اروپا (EU) و ایالت متحده آمریکا (US)، فهرستی از بیانیه‌های کاربردی به‌منظور رعایت شیوه‌نامه‌های کار در منازل، کاهش حملات بدافزارها یا باج‌افزارها، امنیت VPNها و مدیریت ریسک و همچنین، اطمینان از شناسایی و ردیابی چالش‌های مرتبط به کووید ۱۹ را صادر کرده‌اند. مقامات عالی‌رتبهٔ مالی درحال بررسی ریسک‌های امنیت سایبری به‌منظور تداوم فعالیت خدمات مالی هستند. کارمندان مؤسسات مالی مسئول امنیت فناوری

اطلاعات شرکت بوده است و می‌بایست در برابر جرائم سایبری مطلع و آگاه باشند.

افزایش سطح هشدارها از طریق بیانیه‌های عمومی در مورد جرائم سایبری

تعدادی از مقامات عالی‌رتبه بیانیه‌هایی در ارتباط با هوشیار بودن نسبت به افزایش ریسک‌های مرتبط به پولشویی و تروریسم مالی و همچنین هوشیاری کارمندان این مؤسسات در مقابل این قبیل جرائم ارائه کرده‌اند.[۱۷] همچنین تعدادی از مقامات عالی‌رتبه به‌طور عمومی طرح‌های کلی نسبت به حملات سایبری در دوران شیوع کووید ۱۹ را مطرح کرده‌اند. یک نمونه از این مورد مربوط به بیانیهٔ مشترک بانک ایتالیا و مؤسسه سرپرستی بیمه هستند. این دو مؤسسه چالش‌های امنیت سایبری مرتبط به کووید ۱۹ را با تمرکز بر موارد ذیل شناسایی می‌کنند:

- آسیب‌های ناشی از افزایش انجام فعالیت‌ها به‌صورت تلفنی و از راه دور
- انجام بررسی جهت به‌دست آوردن آگاهی‌های لازم برای تهدیدات سایبری در دوران کووید ۱۹

فراهم کردن رهنمودهایی در نواحی انعطاف‌پذیر سایبری

بعضی مقامات رهنمودهایی در مورد افزایش ریسک‌ها در سیستم فناوری اطلاعات عمومی و اطلاعات غیرعمومی ارائه کرده‌اند. به‌عنوان مثال اداره خدمات مالی ایالت نیویورک اعلام کرده است که:

- اهمیت اعتماد به امنیت ارتباطات VPN که تمام تراکنش‌های در حال تبادل را رمزگذاری می‌کند
- به کاربردن پروتکل‌های احراز هویت چند عاملی (مانند شناسنامه، کارت ملی، پاسپورت و...) و به‌روز رسانی آنها برای فعالیت‌های کلیدی
- به‌کاربردن پروتکل‌های امنیتی قوی وسائل شخصی یا خانگی برای دسترسی به زیرساخت‌های تکنولوژیکی شرکت
- تجهیزات و امکانات ویدئویی و کنفرانس‌های صوتی به شیوه‌ای که دسترسی افراد غیرمجاز را محدود کند
- به‌کار بردن معیارهایی به‌منظور جلوگیری از افشای اطلاعات شرکت به‌عنوان بخشی از رهنمود کووید ۱۹ ادارهٔ خدمات مالی ایالت نیویورک از شرکت‌ها درخواست کرده است ریسک‌های مربوط به اشخاص و شرکت‌هایی را که با این شرکت‌ها در ارتباط هستند در این شرایط استثنایی گزارش کنند.

به اشتراک گذاشتن اطلاعات مرتبط به تهدیدات کووید ۱۹

بعضی از مسئولان در حال تبادل اطلاعات مرتبط با تهدیدات سایبری کووید ۱۹ از طریق کانال‌های داخلی با مؤسسات مالی و دیگر همکاران مورد اعتمادشان هستند. سازمان‌هایی از قبیل بانک ایتالیا در حال اشاعهٔ خبرنامه‌های امنیتی، سازماندهی وبینارها و آموزش استفادهٔ صحیح از وسائل شرکت و مستحکم‌تر کردن کنترل‌های مرتبط به کار از راه دور است.

معیارهای ضدپولشویی

گزارش اعضای FSRB و دیگر منابع حاکی از ضعف دولت‌ها در برابر فعالیت‌های ضدپولشویی و ضدتروریسم مالی به‌علت شرایط پیش آمده ناشی از کووید ۱۹ است که این موضوع عمدتاً به‌علت فاصله‌گذاری اجتماعی ناشی از همه‌گیری ویروس کرونا به‌منظور حفظ سلامت مردم و جرائم ناشی از عدم رعایت آن است. بسیاری از کارمندان بخش دولتی ضدپولشویی و ضدتروریسم مالی و همچنین کارمندان بخش خصوصی در حال کار از راه دور هستند یا به‌علت مبتلا شدن به کرونا اصلاً کار نمی‌کنند. به‌طوری‌که در بعضی از کشورها به‌علت کمبود کارمندان ترتیب تقدّم و تأخّر کارها از توجه به فعالیت‌های ضدپولشویی و ضدتروریسم مالی به سمت کارهای دیگر نظیر برقراری ثبات مالی و تلاش برای بهبود شرایط اقتصادی بشریت تغییر پیدا کرده است.

تحقیقات اعضای FATF و محققان دیگر حاکی از توجه به جرائم مالی ایجاد

شده در دوران کووید ۱۹، تأکید بر اهمیت تداوم الزامات ضدپولشویی و ضدتروریسم مالی، مشخص کردن نیاز در به‌کاربردن وسائل نظارتی به شیوه‌ای که رسیدن به تراز بین کاهش پولشویی و تروریسم مالی ایجاد شده ناشی از کووید ۱۹ و انعطاف‌پذیری در مقابل مشکلات کووید ۱۹ را هموار می‌کند.

نتیجه‌گیری

بحران همه‌گیری کرونا زمینهٔ مساعدی را برای جرائم مالی فراهم کرده است. همزمان با شروع همه‌گیری مقامات عالی‌رتبهٔ جهانی با ارائهٔ بیانیه‌ها و رهنمودهایی، به مؤسسات مالی به‌ویژه در مورد کاهش حملات سایبری و ریسک‌های پولشویی و تروریسم مالی پاسخ داده‌اند. مقابله با ریسک‌های پولشویی و تروریسم مالی مستلزم این است که:

۱) مؤسسات مالی و عمومی نسبت به اینگونه جرائم مطلع شوند

۲) توجه بیشتری به ریسک‌های در حال پیدایش داشته باشند

۳) به اشتراک گذاشتن اطلاعات بین مؤسسات عمومی و خصوصی و همچنین بین بخش‌های قضایی

همچنین رهنمودهای صادره تأکید بر انجام معاملات بین مؤسسات مالی به‌منظور افزایش انعطاف‌پذیری سایبری و چهارچوب‌های ضدپولشویی و جلوگیری از تحمیل بار اضافی به مؤسسات مالی در ارائهٔ خدمات مالی دارد. ■

پی‌نوشت‌ها:

1- See eg CERT-EU website https://media.cert.europa.eu/cert/moreclusteredition/en/securityboulevarde65efcacb6cd9b-f31080185461c6e720.20200404.en.html

2- See eg. report in the Financial Times, www.ft.com/content/28b59b28-44ac-43ec-b0dd-c1f1eacfbeb0, and BIS Bulletin, no 3, www.bis.org/publ/bisbull03.pdf, which posits that the outbreak could in principle lead to both higher precautionary holdings of cash by consumers and a structural increase in the use of mobile, card and online payments.

3- Interpol (2020), INTERPOL Warns of Financial Fraud Linked to COVID-19. [online], http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraudlinked - to covid 19

4- US Treasury (2020), COVID-19 Scams, https://home.treasury.gov/services/report-fraud-waste-and abuse /covid - 19- scams.

5- US FDA (2020), There Are No FDA-Approved Drugs Or Vaccines To Treat COVID-19, http://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-testsvaccines- and - treatments

Singapore Police Force (2020), New type of e-commerce scams involving the sale of face masks,, http://www.police.gov.sg/mediaroom/news/20200222_others_new_type_of_ecommerce_scams_involving_the_sale_of_face_masks .

6 - US Justice Department (2020), Darknet Vendor Arrested on Distribution and Money Laundering Charges, https://www.justice.gov/usao-edva/pr/darknet-vendor-arrested-distribution-andmoney-laundering-charges.

- US ICE (2020), ICE HSI arrests Georgia resident for selling illegal pesticide, claiming it protects against coronavirus, https://www.ice.gov/news/releases/ice-hsi-arrests-georgia-resident-selling-illegalpesticide-claiming-it-protects.

7- Europol (2020), COVID-19: Fraud,

17 -See eg MAS media release on regulatory and supervisory measures to help FIs focus on supporting customers, www.mas.gov.sg/news/media-releases/2020/mas-takes-regulatory-and-supervisory-measures-to-help-fis-focus-onsupporting-customers.

-See eg New York State Department of Financial Services Guidance to regulated entities regarding cyber security awareness during Covid-19 pandemic, www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness.

منابع:

- Kristen Alma, Shana Krishnan, Colby Mangels and Mei-Lin Wang. (MAY 2020). COVID-19-related Money Laundering and Terrorist Financing.
- Juan Carlos Crisanto and Jermy Prenio. (MAY 2020). Financial crime in times of Covid-19 – AML and cyber resilience measures , NO. 7.

نسرین عرب بافرانی – دانشجوی دوره کارشناسی ارشد حسابداری

the COVID-19 Pandemic, https://www.austrac.gov.au/smrs-during-covid-19.

13- US Justice Department (2020), Darknet Vendor Arrested on Distribution and Money Laundering Charges, https://www.justice.gov/usao-edva/pr/darknet-vendor-arrested-distribution-andmoney-laundering-charges.

۱۴ - معاملـه در مـورد اوراق بهـادار شـرکت بـا هـدف کسـب سـود یـا جلوگیـری از زیـان (در زمانـی کـه مقامـات درون سـازمان دارای اطلاعاتـی بـه آگاهـی افـراد خـارج از سـازمان برسـد بـر قیمـت اوراق بهـادار شـرکت اثـر خواهـد گذاشـت)

15- UN (2020), Secretary-General's Remarks to the Security Council on the COVID_19 Pandemic, https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-thesecurity-council-the-covid-19-pandemic-delivered.

16- US Treasury (2020), Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of COVID-19 Pandemic, https://home.treasury.gov/news/press-releases/sm969.

http://www.europol.europa.eu/covid-19/covid-19-fraud.

8-US Securities and Exchange Commission (2020), Look Out For Coronavirus-Related Investment Scams - Investor Alert. [online] Available at:, http://www.sec.gov/oiea/investor-alerts-andbulletins/ia_coronavirus.

9- WHO (2020), Cybersecurity. [online] Available at:, http://www.who.int/about/communications/cyber-security.

10- FBI (2020), FBI Anticipates Rise In Business Email Compromise Schemes Related To The COVID-19 Pandemic, http://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-businessemail-compromise-schemes-related-to-the-covid-19-pandemic.

11- Interpol (2020), Cybercriminals Targeting Critical Healthcare Institutions with Ransomware., https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Cybercriminalstargeting-critical-healthcare-institutions-with-ransomware

12- Austrac (2020), Fighting Financial Crime Together – SMRs during