فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال سیزدهم
شمارهٔ دوم، تابستان ۱۳۹۷

عوامل مؤثر بر وقوع جرائم مالی در فضای مجازی؛ با روش تئوری داده بنیان

تاریخ دریافت: ۹۶/۱۰/۱۶ تاریخ پذیرش: ۹۷/۰۲/۳۰

از صفحهٔ ۲۰۹ تا ۲۲۴

رضا قیاسی[۱]، علی رستگار[۲]، صدیقه احمدپور[۳]، بهزاد هادی پور[۴]

چکیده

استفاده روز افزون از فناوری‌های اطلاعات از جمله رایانه و اینترنت، شرایط لازم را برای انواع جرائم سازمان یافته و غیر سازمان‌یافتهٔ اینترنتی فراهم کرده است. روزانه، هزاران نفر در جهان قربانی جرائم سایبری هستند و آگاهی چندانی نیز از انواع جرائم و نحوهٔ وقوع آن‌ها ندارند. در دههٔ ۱۹۹۰ که شبکهٔ جهانی اینترنت فراگیر شد، جرائم رایانه‌ای از جنبهٔ اقتصادی وسیع‌تر شده و ابعاد جدیدتری به خود گرفته است. این مقاله به بررسی و شناسایی عوامل مؤثر بر وقوع جرائم مالی در فضای مجازی و راه‌های پیشگیری از آن می‌پردازد. در این پژوهش، از رویکرد کیفی و با توجه به هدف مطالعه و دستیابی به بررسی نظام‌مند (داده‌های کیفی)، برای جمع‌آوری داده‌ها از مصاحبهٔ نیمه ساخت‌یافته و ابزار پرسش باز و مصاحبه‌های پیاده شده و به طور خاص از روش تئوری داده بنیان استفاده شده است. عملیات اصلی در تجزیه و تحلیل مورد استفاده در تحقیق عبارت است از کدگذاری و یادداشت‌برداری. با توجه به مصاحبه‌های انجام شده، عوامل مختلف اجتماعی، اقتصادی، انسانی و فناورانه (تکنولوژیکی) بر مجرمان تأثیر می‌گذارد تا دست به جرم مالی بزنند؛ این عوامل شامل مواردی از قبیل تورم، بیکاری، گمنامی در فضای مجازی و کسب هویت مجازی، دسترسی به اینترنت، گسترهٔ جهانی داشتن اینترنت، سن، جنس، فقر، وضعیت خانوادگی، گروه همسالان، محیط زندگی فرد و غیره است. با توجه به یافته‌های تحقیق، فیشینگ، اسکیمینگ، فارمینگ و تزریق، بیش‌ترین جرم محسوب می‌شد. ایجاد وب‌سایت‌های جعلی مشابه با سایت قانونی بانک و همچنین استفاده از تلفن و ایمیل از این جهت که افراد را گمراه کرده و در افراد ایجاد نگرانی می‌کنند، قربانیان زیادی دارد. در همین زمینه، براساس یافته‌ها به ارائه پیشنهادهای کاربردی برای کنترل و پیشگیری از جرائم مالی در فضای مجازی پرداخته شده است.

کلید واژه‌ها: فضای مجازی، جرائم مالی، فیشینگ، پیشگیری، تئوری داده بنیان.

استناد: قیاسی، رضا؛ رستگار، علی؛ احمدپور، صدیقه و هادی پور، بهزاد (تابستان ۱۳۹۷). عوامل مؤثر بر وقوع جرائم مالی در فضای مجازی؛ با روش تئوری داده بنیان. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۱۳(۵۰)، صص ۲۲۴-۲۰۹.

۱. عضو هیئت علمی دانشگاه علوم انتظامی امین، rezaghiasi@rocketmail.com
۲. استادیار فناوری اطلاعات دانشگاه علوم انتظامی امین، rastegar1730@chmail.ir
۳. کارشناسی ارشد مدیریت انتظامی دانشگاه علوم انتظامی امین، نویسندهٔ مسئول:
Sedigheh.ahmadpoor1986@gmail.com
۴. عضو هیئت علمی دانشگاه علوم انتظامی امین، B.hadipour96@chmail.ir

مقدمه

نیاز به استفاده روز افزون از رسانه‌های ارتباط‌جمعی مانند اینترنت، علیرغم پیامدهای مثبت و تأثیرگذار فراوان در جامعهٔ امروزی، به دلیل غیربومی بودن دستاوردهای منفی بسیاری نیز داشته و دارد. از جمله این پیامدهای منفی، پیدایش جرائم نوظهور رایانه‌ای و اینترنت است (بویان، جوسانگ و ژو[1]، ۲۰۱۰). استفاده روز افزون از فناوری‌های اطلاعات از جمله رایانه و اینترنت شرایط لازم را برای انواع جرائم سازمان‌یافته و غیر سازمان‌یافته اینترنتی فراهم کرده است. روزانه هزاران نفر در جهان به دلیل اینکه آگاهی چندانی از انواع جرائم سایبری و نحوهٔ وقوع آن‌ها ندارند، قربانی جرائم در فضای سایبر هستند (کاستل[2]،۲۰۱۱). اولین تحقیقاتی که پیرامون جرائم رایانه‌ای صورت گرفت در آمریکا بود که در این تحقیقات، به قضیهٔ کلاهبرداری از طریق سوء استفاده از ۵۶ هزار مورد بیمه به ارزش حدوداً ۳۰ میلیون دلار اشاره کرد. در دههٔ ۱۹۹۰ که شبکهٔ جهانی اینترنت فراگیر شد، جرائم رایانه‌ای از جنبهٔ اقتصادی وسیع‌تر شده و ابعاد جدیدتری به خود گرفت. مطالعات انجام شده نشان می‌دهد که بین سال‌های ۲۰۱۳ تا ۲۰۱۵، تقریباً ۴/۲ میلیون کاربر رایانه در آمریکا به وسیلهٔ فیشینگ زیان دیده‌اند (دیزنین[3]، ۲۰۱۱، ص۲۷).

در کنار جرائم سایبری در حوزهٔ اجتماعی و سیاسی، جرائم سایبری در حوزهٔ اقتصادی پیشرفت‌های قابل‌توجهی داشته است که بنا بر آمار رسمی کشورهای غربی به خصوص آمریکا، جرائم سایبری در حوزهٔ اقتصاد از رتبهٔ بالایی برخوردار است. از سوی دیگر، با توجه به رشد این آمار، پنتاگون در کنار دفاع سایبری در حوزهٔ سیاسی و نظامی، استراتژی مقابله با کلاهبرداری برخط (آنلاین) را نیز از اولویت‌های خود اعلام کرده است (پریشان، ۱۳۹۱). با عنایت به ضرورت توجه به جرائم در فضای مجازی و به ویژه در حوزهٔ جرائم مالی، سئوال اصلی مقالهٔ حاضر این است که عوامل مؤثر بر وقوع جرائم مالی در فضای مجازی کدام‌اند و راه‌های پیشگیری از آن چیست؟

فضای مجازی علاوه بر ویژگی‌های مثبت بسیار، با برخورداری از ویژگی‌های منحصر به فردی همچون بدون مرز بودن، امکان هنجارشکنی را به تمامی نقاط دنیا گسترش داده است. همچنین، با گمنام‌سازی کاربرهای سایبری، امکان شناسایی هویت هنجارشکنان،

1.Bhuiyan, Josang & Xu
2.Castel
3.Denzin

تعقیب و پیگرد آن‌ها را با مشکلات جدی مواجه کـرده اسـت (جلالـی فراهـانی، ۱۳۸۷، ص۲۳). با توجه به شرایطی که در خصوص جرائم ارتکابی در فضای سـایبر وجـود دارد، ضرورت توجه به تدابیر پیشگیرانه برای پلیس دو چندان شده است. لذا همان‌طور که در دنیای فیزیکی رویکرد اصلی به مقولهٔ جرم، پیشگیری از وقوع آن است، در دنیای سـایبر نیز باید به عنوان یک ضرورت مورد توجه قرار گیرد.

امروزه شاهد رشد سرسام‌آور و افزایش تعداد کاربران فضای سایبر و رشد تبادلات مالی و جرائم مالی در این فضا بوده و به دلیل کم بودن دانش و آگاهی عامهٔ مردم در این حوزهٔ نوپا، مجرمان در خیل عظیم کاربران به راحتی قربانی خود را می‌یابنـد. در حـال حاضـر، بالاترین آمار پرونده‌های تشکیل شده در پلیس فتا مربوط به جرائم مالی است و ناشناخته ماندن عوامل مؤثر بر وقوع جرائم مالی در فضای مجازی، روز به روز بر ایـن آمـار افـزوده خواهد کرد (اسکندری پور و همکاران، ۱۳۹۳، ص۴۵). لذا ایـن مقالـه مـی‌توانـد مبـانی نظری و علمی خوبی را فراهم آورده و موجب توسعهٔ دانش در زمینهٔ مبارزه با جرائم مالی در فضای مجازی شده و راهکارهای لازم را برای کاهش این جرائم ارائه کند.

پژوهش‌های مختلفی از زمان ظهور جرائم در فضای مجازی در سطح داخلی و خارجی در حوزه‌های مختلف جرائم سایبری صورت گرفته است. محمدیان (۱۳۹۱) در پایان‌نامهٔ کارشناسی ارشد با عنوان «بررسی پیشگیری از جرائم رایانه‌ای و شیوه‌های آن» با تکیه بر مدل پیشگیری غیرکیفری و کیفری، سعی در تبیین و بررسـی روش‌هـای پیشـگیری از وقوع جرائم رایانه‌ای داشته و راهکارهای متعددی را جهـت اجـرای کـاربردی روش‌هـای مذکور ارائه کرده است. محقق در نهایت به ایـن نتیجـه رسـیده کـه نگـرش تـک‌بعـدیِ واکنشی جهت پیشگیری از جرائم مذکور کافی نبوده و باید مجموعه‌ای از اقدامات کنشی و واکنشی از سوی نهادهای ذی‌ربط به صورت نهادینه و علمی اجرا شود. ملکـی (۱۳۹۶) نیز در پایان‌نامهٔ خود تحت عنوان «شناسایی روش‌های نوین کلاهبرداری مالی در فضای سایبر و ارائه راهکارهـای پیشـگیرانه»، بـیش‌تـرین تـأثیر در پیشـگیری از وقـوع جـرائم کلاهبرداری مالی سایبری را افزایش سواد فناوری اطلاعات در میان کاربران دانسته است. همچنین، خصوصیات و ویژگی‌های شخصیتی مجرمان و عدم بازار کار مناسـب و انتظـار درآمد مالی در رتبه‌های بعدی قرار دارد.

شاه‌محمدی و تاهو (۱۳۹۳) مقاله‌ای با عنوان «بررسی شیوه‌های پیشـگیری از جـرائم سایبری؛ مبتنی بر فناوری اطلاعات»، با هدف تبیین شیوه‌های ارتکاب جرائم سـایبری و

نحوهٔ پیشگیری از آن انجام داده‌اند که نتایج آن نشان می‌دهد شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت فضای مجازی و کنترل و نظارت بر فضای مجازی، جمع‌آوری ادلهٔ الکترونیکی جرم و مستندسازی صحنهٔ جرم در پیشگیری از جرائم سایبری تأثیر دارد. همچنین، کمالی‌زاده و شاه‌محمدی (بهار ۱۳۹۵)، در پژوهشی با عنوان «ارزیابی روش‌های شناسایی وب‌سایت فیشینگ»، ضمن معرفی حمله فیشینگ و روش‌های موجود، به این نتیجه رسیده‌اند روش‌هایی که از تکنیک‌های مختلف شناسایی در کنار هم استفاده می‌کنند و اکثر ویژگی‌های صفحات وب را بررسی می‌کنند، در شناسایی حمله از موفقیت بیشتری برخوردار می‌باشند.

جرائم مالی سایبری: واژهٔ سایبر از نظر لغوی به معنای مجازی و غیرملموس است. به عبارت دیگر، سایبر به مطالعهٔ مکانیزم‌های مورد استفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود. اصطلاح فضای سایبر یا دنیای مجازی برخط (آنلاین)، اصطلاحی است که نخستین بار توسط ویلیام گیبسون در رمانی با عنوان نیورومانسو در سال ۱۹۸۴ مورد استفاده قرار گرفت (سید مفیدی، ۱۳۸۳، ص۹۸). جرائم مالی نیز جزئی از جرائم سایبری هستند که با سوء استفاده از اعتماد مال‌باختگان با استفاده از مهندسی اجتماعی، فیشینگ و تزریق بدافزارها، اقدام به برداشت غیرمجاز از حساب بزه‌دیده‌ها می‌شود. همچنین، فیشینگ تکنیک شناخته شده‌ای است که با ایجاد وب‌سایت‌های جعلی طراحی شده، مشابه یک سایت قانونی بانک یا مؤسسهٔ مالی و با استفاده از روش‌های هرزه‌نگاری سیستمی جهت موجه و قانونی جلوه دادن به استفاده‌کنندگان می‌پردازد (صادقی، ۱۳۹۱، ص۴۸).

با توجه به تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی (۱۳۸۸) و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون افتای دولت مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات (فتا)، این پلیس در بهمن‌ماه ۱۳۸۹ به دستور فرماندهی نیروی انتظامی تشکیل شد (بوربور، ۱۳۹۵، ص۸۵) که علاوه بر پی‌جویی و کشف جرائم سایبری، پیشگیری از وقوع جرائم در این فضا نیز در دستور کار قرار داده است. واژهٔ پیشگیری از نظر اصطلاحی، یعنی اقدامات احتیاطی برای جلوگیری از رخدادهای بد و ناخواسته و پیشگیری از جرم، هر عملی که باعث کاهش بزهکاری، خشونت، ناامنی از طریق مشخص کردن و حل کردن عوامل ایجاد کنندهٔ این مشکلات به روش علمی شود (زینالی، ۱۳۸۳، ص۶۳).

نظریهٔ پیشگیری وضعی از جرائم کلاهبرداری فضای مجازی: یکی از شیوه‌های پیشگیری غیر کیفری مؤثر در کاهش جرائم علی‌الخصوص جرائم سایبری، پیشگیری وضعی است و در کشورهای پیشرفته، تمرکز و سرمایه‌گذاری خاصی در بررسی شیوه‌های پیشگیری وضعی انجام یافته است. جرائم سایبری اغلب بر پایهٔ فناوری اطلاعات به وقوع می‌پیوندند و روال‌های مجرمانهٔ آن‌ها در فضای مجازی سپری می‌شود، لذا رویکردهای پیشگیرانه مبتنی بر فناوری اطلاعات می‌تواند عامل مؤثری در پیشگیری از وقوع و ارتکاب جرائم سایبری باشد. متناسب با پیشرفت و پیچیده‌تر شدن جرائم سایبری، راهکارهای پیشگیری مبتنی بر فناوری اطلاعات نیز باید بروز رسانی شوند. یکی از نظریه‌های مطرح در زمینهٔ پیشگیری وضعی، نظریهٔ اندرسون است که در چهار بخش و ۱۶ مؤلفه عنوان شده است (اندرسون[1]، ۲۰۱۳، ص۶۸). رابسون نیز معتقد است وقتی فرد، داغ ننگین بر پیشانی دارد، در تعامل و ارتباطات خود با دیگران از عهدهٔ حل مسائل و مشکلات ناشی از آن برنمی‌آید، در نتیجه به رفتار انحرافی خود ادامه می‌دهد ۲۰۱۲، ص۱۷). یکی دیگر از نظریه‌های مطرح در زمینهٔ پیشگیری وضعی، نظریهٔ رونالد کلارک است که در چهار بخش اصلی و هر بخش، به چهار تکنیک یا راهکار تقسیم شده است؛ بخش اول، افزایش تلاش (زحمت) مورد نظر است. بخش دوم، افزایش خطرات مورد نظر برای ارتکاب جرم مانند دستگیری یا شناخته شدن مرتکب است. بخش سوم شامل کاهش دستاوردهای مورد انتظار از جرم یا همان سود حاصله و بخش چهارم، حذف بهانه‌ها یا از بین بردن عواملی که باعث تحریک یا تشویق فرد به ارتکاب جرم می‌شود، است (هیوز، ۱۳۸۳، ص۱۴۵).

روش‌شناسی تحقیق

این پژوهش، از رویکرد کیفی بهره‌مند شده است و تأکید بر دیدگاه مشارکت‌کنندگان در پژوهش به عنوان منبع اصلی داده‌های پژوهشی است. روش خاص موردنظر، روش گرندد تئوری یا روش داده بنیان است. منظور از تئوری داده بنیان، نظریه‌های برگرفته از داده‌هایی است که در طی فرآیند پژوهش به‌صورت نظام‌مند گردآوری و تحلیل شده‌اند. در این راهبرد، گردآوری و تحلیل داده‌ها و نظریه‌ای که در نهایت از داده‌ها استنتاج

1.Anderson
2.Robson

می‌شود، در ارتباط نزدیک با یکدیگر قرار دارند. پژوهشگر به جای اینکه مطالعهٔ خود را با نظریهٔ از پیش تصور شده‌ای آغاز کند، کار را با یک حوزهٔ مطالعاتی خاص شروع کرده و اجازه می‌دهد که نظریه از دل داده‌ها پدیدار شود. نظریهٔ برگرفته از داده‌ها نسبت به نظریه‌ای که حاصل جمع آمدن یک سلسله مفاهیم براساس تجربه یا تأملات صرف است، با احتمال بیشتری می‌تواند نمایانگر واقعیت باشد و از آنجا که نظریه‌های زمینه‌ای از داده‌ها استنتاج می‌شوند، می‌توانند با ایجاد بصیرت و ادراک عمیق‌تر، رهنمود مطمئنی برای عمل باشند (ابوالمعالی، ۱۳۹۱، ص۱۵). جامعهٔ آماری تحقیق را کلیهٔ افراد شهر تهران که دارای پروندهٔ سرقت جرائم مالی در پلیس فتا هستند، تشکیل می‌دهد که این افراد طی سال ۹۴ به دادسرای ناحیهٔ ۳۱ تهران مراجعه و تشکیل پرونده کرده‌اند. شیوهٔ نمونه‌گیری در پژوهش‌های کیفی، نمونه‌گیری هدفمند است که به آن نمونه‌گیری غیراحتمالی، هدف‌دار یا کیفی نیز می‌گویند و به معنای انتخاب هدف‌دار واحدهای پژوهش برای کسب دانش یا اطلاعات است. روش نمونه‌گیری در این پژوهش، هدفمند قضاوتی است و با ابزار مصاحبهٔ عمیق نیمه ساختار یافته با ۱۰ نفر از افراد قربانی جرائم مالی و ۷ نفر از مجرمان جرائم مالی پژوهش صورت گرفته است. مصاحبه‌های نیمه ساخت‌یافته بیش از انواع دیگر مصاحبه‌ها به تفاهم بین مصاحبه‌کننده و مصاحبه‌شونده بستگی دارد. عملیات اصلی در تحلیل داده‌ها به روش تئوری داده بنیان عبارتند از: کدگذاری و یادداشت‌برداری. منظور از کدگذاری اختصاص نام و برچسب به قطعاتی از داده‌های جمع‌آوری شده است و یادداشت‌برداری به فرآیند پژوهش وضوح می‌بخشد و منجر به تصمیمات تحلیلی مناسب شده، تحلیل داده‌ها را گسترش داده و چهارچوبی برای تبیین و تدوین نظریه ایجاد می‌کند (ابوالمعالی,۱۳۹۰، صص۶۵-۶۸). اعتبار در پژوهش کیفی به این موضوع اشاره دارد که تا چه اندازه واقعیت‌ها یا حقایق ابراز شده توسط افراد مورد مطالعه به درستی توسط پژوهشگر منعکس شده است. برای وارسی این ملاک ارزیابی از دو روش استفاده شد؛ اول، با استفاده از فن وارسی عضو که طی آن برداشت‌های پژوهشگر با مصاحبه‌شونده در میان گذاشته می‌شود تا صحت و سقم آن‌ها مشخص شود. دوم، داده‌ها توسط دو تحلیل‌گر مورد تحلیل قرار گرفتند تا اثرت برداشت‌ها و سوگیری‌های شخصی به حداقل برسد. برای روایی بیش‌تر، پژوهشگر با دادن وقت کافی به پاسخ‌دهندگان و تفهیم لازم در مورد سؤال‌ها و رفع ابهام در خصوص پرسش‌ها تا حد امکان و با سعهٔ صدر لازم به تعامل با آزمون‌های موردنظر مبادرت ورزیدند.

یافته‌های تحقیق

با مصاحبه‌هایی که از قربانیان جرائم مالی صورت گرفت، مقوله‌هایی شناسایی شد کـه از کدگذاری داده‌های به دست‌آمده ایجاد شد و در جدول ۱ نشان داده شده است.

جدول ۱ – یافته‌های منتج از مصاحبه با قربانیان جرائم مالی فضای مجازی

مقوله‌ها	کدها	
فیشینگ	وب‌سایت جعلی	لوگوها و تصاویر ساختگی، عدم آگاهی، ایجاد پیام به صورت غیرمنتظره
	تلفن	پیام دادن از طرف بانک جعلی، اعلام مشکل، ایجاد نگرانی و رفع مشکل توسط تماس سریع
	ایمیل	استفاده از لوگوها و علائم تجاری مؤسسه‌های بانکی
اسکیمینگ	دستگاه کارت‌خوان	دادن رمز به افراد غریبه، فاش کردن اطلاعات حساب
	ایجاد صفحهٔ قلابی	ایجاد صفحات جعلی، اسکیمرها، عدم آگاهی
فارمینگ		وجود هکرها و ثبت اطلاعات، شباهت زیاد با سایت اصلی، عدم آگاهی
تزریق		کلاهبرداری در سهام، تهدید از طریق ایجاد هرزنامه، افزایش سهام به طور غیرواقعی، فروش آن به خریداران کم‌تجربه، هک کردن بانک اطلاعاتی خریدار

برای قربانیان جرائم مالی، چهار نوع جـرم کـه دارای بـیش‌تـرین وقـوع بـوده اسـت، شناسایی شد. فیشینگ، اسکیمینگ، فارمینگ و تزریق. برای هرکدام از این عامل، عوامل مختلف دیگری شناسایی شده‌اند. فیشینگ که خـود شـامل اسـتفاده از وب‌سـایت‌هـای جعلی، فیشینگ از طریق تلفن و فیشینگ از طریق ایمیل است. وب‌سـایت‌هـای جعلـی خود عواملی مانند لوگوهـا و تصـاویر سـاختگی، عـدم آگـاهی، ایجـاد پیـام بـه صـورت غیرمنتظره را شامل می‌شدند که سبب فریب دادن افراد می‌شدند. تلفـن خـود از طریـق عواملی مانند پیام دادن از طرف بانک جعلی، اعلام مشکل، ایجاد نگرانـی و رفـع مشـکل توسط تماس سریع، سبب فریب مردم می‌شود. آخـرین مـورد در فیشـینگ، اسـتفاده از ایمیل است که خود از طریق استفاده از لوگوها و علائم تجاری مؤسسه‌های بانکی سـبب فریب دادن و ایجاد جرم می‌شود.

در حالت اسکیمینگ، دو نوع روش که شامل استفاده از پوزهای دستگاه کارت‌خوان و ایجاد صفحه کلید قلابی بر روی عابر بانک است. در مورد پوزهای دسـتگاه کـارت‌خـوان، دادن رمز به افراد غریبه و فروشنده و همچنین فاش کـردن اطلاعـات حسـاب از عوامـل ایجاد جرم محسوب می‌شد و سبب فریب خوردن افراد شد. همچنین، ایجاد صفحه کلید قلابی شامل ایجاد صفحات جعلی، وجود اسکیمرها و عـدم آگـاهی از آن عـاملی بـود تـا سبب فریب خوردن و قربانی شدن افراد شود. در روش فارمینگ، وجـود هکرهـا و ثبـت اطلاعات، شباهت زیاد با سایت اصلی و عدم آگاهی افراد، زمینه‌ای برای قربانی شدن این

جرم شده و مالباخته شوند. همچنین، در تزریق، یکی از روش‌های پرکاربرد، کلاهبرداری در سهام است که تهدید از طریق ایجاد کمپین هرزنامه، افزایش سهام به طور غیرواقعی و فروش آن به خریداران کم‌تجربه و هک بانک اطلاعاتی خریدار ازجمله عواملی است که سبب مال‌باختگی قربانیان و فریب خوردن آن‌ها می‌شود.

در بخش دیگری از تحقیق با مصاحبه‌هایی که با ۷ نفر از مجرمان جرائم مالی صورت گرفت، به منظور پاسخگویی به سؤال‌های پژوهش، مصاحبه‌ها آماده‌سازی و تحلیل شد. تحلیل کیفی داده‌ها در هر نمونه به‌طور مجزا انجام شد و مقوله‌های دیگری شناسایی شد که از کدگذاری داده‌های به دست آمده ایجاد شد و در جدول ۲ نشان داده شده است.

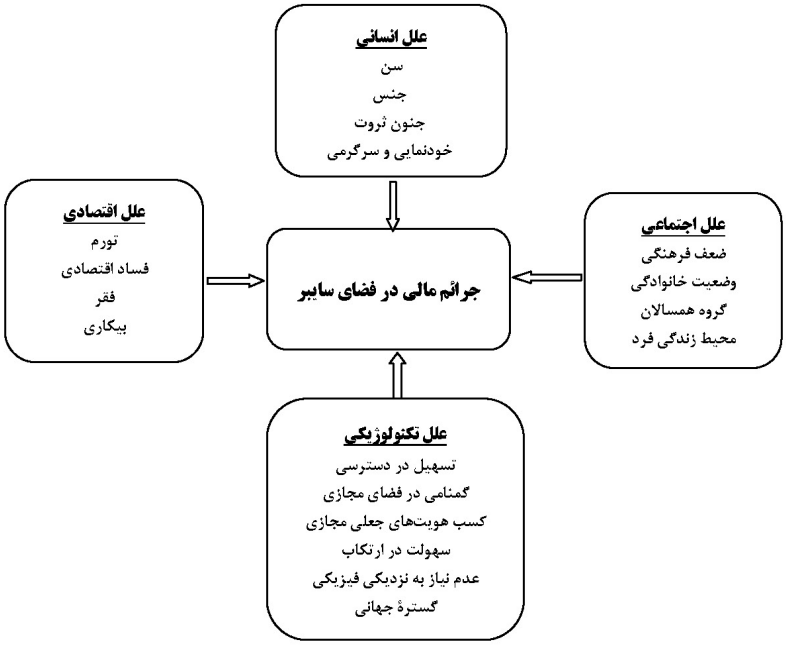
جدول ۲ – مصاحبه با مجرمان جرائم مالی و عوامل مؤثر بر ارتکاب جرم فضای مجازی

مقوله‌های اصلی	کدها	
عوامل اجتماعی	وضعیت خانوادگی	اعتیاد والدین، درآمد پایین، راحتی در گرفتن اطلاعات حساب دیگران
	گروه همسالان محیط زندگی فرد	تشویق دوستان، الگو گرفتن از بهترین دوست، لذت بردن از فضای مجازی و اخاذی از مردم، امکانات بیش از حد، وجود اینترنت، لذت بردن از سوء استفاده از مردم
عوامل فناورانه (تکنولوژیکی)	گسترهٔ جهانی اطلاعات از کل جهان، گمنامی در فضای مجازی، کسب هویت‌های جعلی مجازی، استفاده از فناوری‌های روز جهان، عدم نیاز به نزدیکی فیزیکی، دسترسی آسان، عمل جرم در خانه و هر مکان دیگری	
عوامل انسانی	سن‌سنین بالا، درک موقعیت، هوشمندی زیاد، تجربه کاری بالا	
	جنسیت، عدم ترس و دلهره در مردان، انجام عمل در هر مکان و موقعیت	
عوامل اقتصادی	فقر و تنگدستی، عشق پولدار شدن، عدم رضایت از زندگی، تحصیلات بالا و عدم وجود شغل، معضل بیکاری و نبود سابقهٔ کاری، غیرمرتبط بودن کار با رشتهٔ تحصیلی، افسردگی، فشار تورم و سختی زندگی، حقوق پایین و کفایت نکردن حقوق برای زندگی	

در نمونهٔ مربوط به مجرمان، عواملی که سبب ایجاد جرم توسط مجرمان شده است شامل عوامل اجتماعی از قبیل وضعیت خانوادگی، گروه همسالان و محیط زندگی فرد است؛ وضعیت خانوادگی شامل اعتیاد والدین، درآمد پایین، راحتی در گرفتن اطلاعات حساب دیگران؛ گروه همسالان شامل تشویق دوستان، الگو گرفتن از بهترین دوست، لذت بردن از فضای مجازی و اخاذی از مردم و محیط زندگی فرد شامل امکانات بیش از حد، وجود اینترنت و لذت بردن از سوءاستفاده از مردم را شامل می‌شود.

عوامل فناورانه (تکنولوژیکی)، گسترهٔ جهانی، گمنامی و کسب هویت‌های جعلی مجازی، دسترسی به اطلاعات از کل جهان، استفاده از فناوری‌های روز جهان، عدم نیاز به نزدیکی فیزیکی، دسترسی آسان و انجام عمل جرم در خانه و هر مکان دیگری را شامل می‌شود. عوامل انسانی نیز سن (سنین بالا، درک موقعیت، هوشمندی زیاد و تجربهٔ

کاری بالا و جنس (عدم ترس و دلهره در مردان و انجام عمل در هر مکان و موقعیت) را شامل می‌شود. همچنین، عوامل اقتصادی، فقر (تنگدستی، عشق پولدار شدن، عدم رضایت از زندگی)، بیکاری (تحصیلات بالا و عدم وجود شغل، معضل بیکاری و نبود سابقهٔ کاری، غیر مرتبط بودن کار با رشتهٔ تحصیلی)، افسردگی و تورم (فشار و سختی زندگی، حقوق پایین و کفایت نکردن حقوق برای زندگی) را شامل می‌شود.



شکل ۱ – مدل مفهومی تحقیق

بحث و نتیجه‌گیری

از ویژگی‌های خاص این پژوهش، اتخاذ رویکرد پدیدار شناختی و بررسی موضوع از دیدگاه افراد درگیر در موضوع مورد مطالعه بود. در موضوعاتی که جنبه‌های فرهنگی نقش مهمی ایفا می‌کند، استفاده از یافته‌های پژوهش‌های خارجی چندان مفید واقع نمی‌شود. ویژگی مهم دیگر، جامعیت پژوهش حاضر است که سعی در بررسی تمامی جنبه‌هایی بود که سبب ایجاد جرم توسط مجرمان و همچنین عواملی که قربانیان به آن اشاره کرده‌اند، است که حتی در پژوهش‌های کیفی داخلی کمتر به آن توجه شده بود. تأکید بعدی بر نمونه پژوهش بود که قربانیان جرائم مالی در نظر گرفته شد؛ از این جهت که چطور مورد حمله مجرمان قرار گرفتند. از طرفی، سعی شد تا عواملی که سبب ایجاد

جرم توسط مجرمان می‌شود نیز از دیدگاه خود مجرمان مورد بررسی قرار گیرد. در واقع، در این پژوهش دو نمونه بررسی شد: قربانیان جرائم مالی و مجرمان جرائم مالی.

با توجه به مصاحبه‌های انجام شده توسط افراد قربانی و افراد مجرم، مشخص شد که سایبر محیطی است مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی، این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند. در این محیط، تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر آنچه در کرهٔ خاکی به صورت فیزیکی و ملموس یعنی نوشته، تصویر، صوت، اسناد و غیره وجود دارد، در یک فضای مجازی نیز به شکل دیجیتالی وجود دارد و قابل استفاده و در دسترس کاربران از طریق رایانه و شبکه‌های بین‌المللی به هم مرتبط است. امنیت ناکافی فناوری همراه با طبیعت مجازی آن، فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران کننده‌ترین جنبهٔ فضای سایبر، انتشار سریع اطلاعات در آن است؛ برای مثال، در لحظهٔ کوتاهی قسمتی از اطلاعاتی که می‌تواند به طور بالقوه مورد سوء استفاده قرار گیرد، کشف می‌شود. در فضای سایبر برای جستجو و پیداکردن این جرائم، مشکلات پیچیده‌تر می‌شود. در دنیای واقعی، دزدی از بانک اقدامی کاملاً مشخص است؛ چراکه بعد از سرقت در خزانهٔ بانک پولی موجود نیست، ولی با توسل به فناوری، یک خزانه می‌تواند بدون هیچ علامتی خالی شود. برای مثال، سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را به همان صورت قبل باقی بگذارد. در فضای سایبر کپی درست همانند اصل است. با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی را تغییر دهد. کلاهبرداران همیشه در حال تغییر روش‌های خود هستند، در نتیجه شهروندان باید با تیزهوشی، مانع از رسیدن آن‌ها به اهداف خود شوند. یک روش تبهکاران آن است که اطلاعاتی نظیر کلمهٔ کاربری، رمز عبور، شمارهٔ شانزده رقمی عابر بانک، رمز دوم و کد اعتبار سنجی[1] را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند. شبکه‌های اجتماعی، سایت‌های حراجی و درگاه‌های پرداخت برخط (آنلاین)، نمونه‌ای از ابزارهای الکترونیکی ارتباطات است. همچنین، کلاهبرداری گاه از طریق ایمیل‌ها و پیام‌ها صورت می‌گیرد و قربانیان به صورت مستقیم اطلاعات حساس و

1.Card Verification Value (CVV2)

محرمانهٔ خود را در وب‌سایت‌های جعلی که در ظاهر کاملاً شبیه وب‌سایت‌های سالم و قانونی است، وارد می‌کنند.

با توجه به مصاحبه‌های انجام شده، فیشینگ، اسکیمینگ، فارمینگ و تزریق، بیش‌ترین جرم محسوب می‌شود. ایجاد وب‌سایت‌های جعلی مشابه با سایت قانونی بانک و همچنین استفاده از تلفن و ایمیل از این جهت که افراد را گمراه کرده و در افراد ایجاد نگرانی می‌کنند، قربانیان زیادی دارد. پیامک دادن به افراد و پیگیری افراد از طریق یک شماره و در منزل و در هر مکان دیگری، سریع‌ترین و راحت‌ترین روشی است که اطلاعات حساب افراد در اختیار مجرمان قرار خواهد گرفت. استفاده از دستگاه‌های پوز و در اختیار قرار دادن رمز کارت و رمز عبور به دست هر فروشنده و در بین افراد مختلف، روشی ساده برای از دست دادن اطلاعات است. همچنین، عوامل مختلف اجتماعی، اقتصادی، انسانی و فناورانه بر مجرمان تأثیر می‌گذارد تا دست به جرم مالی بزنند. عواملی از قبیل تورم، بیکاری، دسترسی به اینترنت، گسترهٔ جهانی داشتن اینترنت، سن، جنس، فقر، وضعیت خانوادگی، گروه همسالان، محیط زندگی فرد و غیره عوامل زیادی هستند که بر مجرمان تأثیر گذاشته و سبب ایجاد جرم می‌شوند. این بخش از نتایج تحقیق با یافته‌های تحقیق محمدیان (۱۳۹۱) که مجموعه‌ای از اقدامات کنشی و واکنشی را به جای نگرش تک‌بعدی به جرائم حوزهٔ فضای مجازی اعلام کرده است، همخوانی دارد.

یکی دیگر از علل گرایش افراد به ارتکاب جرائم مالی در فضای مجازی را می‌توان خودنمائی و سرگرمی و تفریح ذکر کرد. همچنین، افراد صرف نمایش استعدادهای خود از گستردگی و امکانات فضای مجازی استفاده کرده، مرتکب این جرائم می‌شوند؛ به‌طوری که هک کردن یک سیستم و دسترسی به داده‌های سایر افراد برایشان جذابیت داشته و افتخارآمیز است. لذا پیشنهاد می‌شود دولت با شناسایی این افراد و استعدادیابی و با برنامه‌ریزی صحیح و بهره‌گیری از استعداد و توانایی این افراد در جهت پیشرفت کشور و با جهت دادن به توانایی‌های این افراد، از بروز جرائم جلوگیری کند.

علت دیگری که می‌توان بیان کرد، فقر اقتصادی، بیکاری و عدم تطابق مخارج و درآمد افراد است و فضای مجازی برای این افراد بهترین گزینه برای ارتکاب جرم مالی است. لذا افراد با توجه به عدم آگاهی بسیاری از افراد از فناوری و همچنین وجود ضعف در سیستم بانکداری و همچنین عدم نیاز به رابطهٔ نزدیک و فیزیکی بین قربانی و مجرم، از این روش جهت ارتکاب جرم استفاده می‌کنند. لذا پیشنهاد می‌شود دولت با به‌کارگیری تدابیر لازم

در خصوص رفع معضل بیکاری اقدام کرده و به فکر معاش افراد جامعه باشد تا با تـأمین نیاز اقتصادی، از وقوع این جرائم جلوگیری کند. این نتیجه با یافته‌های ملکی (۱۳۹۶) در مورد عدم بازار کار مناسب و انتظارات درآمد مالی از طرف مجرمان همخوانی دارد.

یکی دیگر از علل وقوع جرم مالی در فضای مجازی را می‌تـوان گمنـامی در ایـن فضـا و کسب عناوین جعلی مجازی و گسـتردگی ایـن فضـا و دسترسـی آسـان بـه اطلاعـات و ناشناس ماندن یا مخفی شدن بعد از وقوع جرم دانست که بهترین حسن از نظر مجرمان محسوب می‌شود. لذا پیشنهاد می‌شود دسترسی افراد ناشناس به اینترنت کنترل شـود و میزان دسترسی آن‌ها به پهنای باند اینترنتـی و حرفـه‌ای محـدود شـود و همچنـین بـا محدودسازی استفاده از فیلترشکن توسط کاربران جهت مخفی کردن و ناشـناس مانـدن جلوگیری شود تا از بروز اینگونه جرائم جلوگیری شود.

علت دیگر وقوع جرائم مالی مجازی، ضعف اطلاعـاتی برخـی از خـدمات الکترونیکـی بانک‌ها و عدم تجهیز دستگاه‌های خودپرداز (ATM[1]) بانک‌ها به سیستم آنتـی اسـکیمر است که مجرمان با سوءاستفاده از این نقص، اقدام به هک سیستم بانکی کرده یا با نصب کردن اسکیمرها بر روی دستگاه‌های خودپرداز، اقدام به جرم مالی می‌کنند که پیشـنهاد می‌شود با هماهنگی لازم با بانک مرکزی و الزام مجهز کردن کلیهٔ دستگاه‌های خودپرداز بانک‌ها به سیستم ضد اسکیمینگ و همچنین سیستم بانکداری الکترونیکی، از وقوع این جرائم جلوگیری کرده و فرصت ارتکاب جرم از مجرمان گرفته شود.

پیشنهادهای کاربردی:

- در خصوص بالا بردن سطح آگاهی والدین و محدودسازی میزان دسترسی فرزندانشـان به اینترنت و همچنین آموزش عمومی افراد جامعه از طریـق رسـانه‌هـای جمعـی ماننـد تلویزیون در خصوص ابزار الکترونیکی و دانش مجازی اقدام شود.

- به هیچ وجه و به هیچ عنوان به آدرس ارسال‌کننـدهٔ ایمیـل اعتمـاد نشـود؛ اگرچـه در برخی سرویس‌هایی اینترنتی، آدرس ایمیل‌های تقلبی تا حدودی تشخیص داده می‌شوند.

- شهروندان باید شخصاً از دستگاه کارت خوان استفاده و رمز عبور را وارد کنند و به آن‌ها توصیه می‌شود تا هنگام استفاده از این دستگاه باید توجه داشته باشند، قطعات اضـافی و مشکوک به منظور پیشگیری از تخلفات سایبری توسط اسکیمرها به آن متصل نباشد.

1. Automated Teller Machine (ATM)

- موجودی حساب‌های بانکی به خصوص حساب‌های عابر بانک را در فاصله‌های زمانی مناسب چک شده و از ارائه اطلاعات بانکی از جمله شماره حساب، شماره کارت‌ها و رمز دوم به سایت‌های متفرقه خودداری شود.
- ارائه طرحی در خصوص جمع‌آوری لاگ فایل[1] خدمات دهندگان اینترنتی از قبیل PAP، ISDP، ISP، کافی‌نت‌ها و مراکز حساس مرتبط با تراکنش‌های مالی نظیر بانک‌ها و مؤسسه‌های مالی.
- جمع‌آوری اطلاعات و بررسی کارآیی سامانه‌ها و ابزارهای ضدفیشینگ و ضدفارمینگ و ارائه طرحی در خصوص پیاده‌سازی آن‌ها به‌صورت بومی در داخل کشور.
- طراحی و پیاده‌سازی پروتکل‌های امن نظیر DNSSEC[2] و برآورد سیاست‌های پیاده‌سازی آن‌ها.
- طراحی و پیاده‌سازی آنتی‌ویروس و فایروال بومی کشور.

منابع

منابع فارسی

- ابوالمعالی، خدیجه (۱۳۹۱). *پژوهش کیفی از نظریه تا عمل*. تهران: نشر علم.
- اسکندری پور، شهرام؛ مقدمی، ایرج؛ امیری، نصرت اله و شاه‌محمدی، غلامرضا (زمستان ۱۳۹۲). بررسی عوامل و راهکارهای مؤثر بر کاهش برداشت‌های غیرمجاز اینترنتی. *فصلنامهٔ دانش انتظامی زنجان*. ۳(۹)، صص۱-۱۱. بازیابی از: http://yon.ir/8McVl
- اعلایی، مهدی (۱۳۹۵). *کلاهبرداری اینترنتی، ابزارها و راهکارهای پیشگیری از آن*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ مدیریت فناوری. دانشگاه آزاد اسلامی واحد الکترونیکی.
- پریشان، جابر (آبان ۱۳۹۱). *بررسی جرم کلاهبرداری رایانه‌ای*. پایگاه اطلاع‌رسانی حقوق ارتباطات. بازیابی از: http://cl-m.mihanblog.com/post/130
- جلالی فراهانی، امیرحسین (تابستان ۱۳۸۳). پیشگیری از جرائم رایانه‌ای، *مجلهٔ حقوقی دادگستری*. ۱۴(۴۷)، صص۸۷-۱۲۰. بازیابی از: https://www.noormags.ir/view/fa/articlepage/484415

1.Log file
2.Domain Name System Security Extensions

- حافظ نیا، محمدرضا (۱۳۹۲). *مقدمه‌ای بر روش تحقیق در علوم انسانی*. تهران: انتشارات سمت.

- زینالی، حمزه (۱۳۸۱). پیشگیری از بزهکاری و مدیریت آن در پرتو قوانین و مقررات جاری ایران. *فصلنامهٔ رفاه اجتماعی*. ۲(۶)، صص۷۶-۸۳. بازیابی از: http://yon.ir/C6MGO

- شاه محمدی، غلامرضا و تاهو، منصور (پاییز ۱۳۹۳). بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۹(۳۵)، صص۹۹-۱۲۰. بازیابی از: http://yon.ir/n5vbk

- صادقی، حمید. (۱۳۹۱) *مطالعهٔ جامع در مورد جرائم سایبری*. تهران: پلیس فتا ناجا.

- کمالی‌زاده، سلمان و شاه‌محمدی، غلامرضا (بهار ۱۳۹۵). ارزیابی روش‌های شناسایی وب‌سایت فیشینگ. فصلنامهٔ *پژوهش‌های اطلاعاتی و جنایی*. ۱۱(۴۱)، صص ۹-۳۸. بازیابی از: http://yon.ir/II0tY

- محمدیان، تقی (۱۳۹۱). بررسی پیشگیری از جرائم رایانه‌ای و شیوه‌های آن. پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق جزا. دانشگاه قم.

- مدیری، علی (۱۳۹۳). *نقش رسانه‌ها در بزهکاری و پیشگیری از آن*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق جزا. دانشگاه قم.

- مسعود، بوربور (۱۳۹۵). *شیوه‌های نوین برداشت‌های مالی در فضای مجازی*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ مدیریت فناوری اطلاعات. دانشگاه علوم انتظامی امین.

- ملکی، امین (۱۳۹۶). *شناسایی روش‌های نوین کلاهبرداری مالی در فضای سایبر و ارائه راهکارهای پیشگیرانه*. پایان‌نامهٔ کارشناسی ارشد رشتهٔ مدیریت فناوری اطلاعات. دانشگاه آزاد اسلامی واحد الکترونیکی تهران.

- هیوز، گوردون (۱۳۸۰). *پیشگیری از جرم؛ کنترل اجتماعی، ریسک و مدرنیتهٔ اخیر* (علیرضا کلدی، محمدتقی جغتایی، مترجمان). تهران: انتشارات سازمان بهزیستی کشور.

منابع انگلیسی

- Anderson, Keith, B. (2013).Consumer Fraud in the United States, 2011: The Third FTC Survey, Staff Report of the Bureau of Economics Federal Trade Commission. Retrieved from: http://yon.ir/Thd7T

- Castel, winkler (2011). Securing the Cloud, Cloud Computer Security Techniques and Tactics.

- Denzin, N. K., & Lincoln, Y. S. (Eds.) (2011). Handbook of qualitative

research (3rd ed.). Thousand Oaks, CA: Sage.
- Bhuiyan, T., Josang, A., Xu, Y. (springer 2010). Managing Trust in Online Social Networks. In B. Furht (Eds) handbook of social network technologies and applications (497 – 471). Heidelberg. Retrieved from: *http://yon.ir/Tu9TO*
- Robson, Rosina (2012). Cyber security and fraud: the impact on small businesses, Federation of small business. Retrieved from: *http://yon.ir/o2Ofw*