مقاله علمی – پژوهشی

# تحلیل توزیع مکانی قربانیان جرم برداشت غیرمجاز از حساب‌های بانکی در شهر تهران

وحید بارانی پسیان[1]، محمدرضا پورغلامی سروندانی[2]، سیدعلی عبادی‌نژاد[3]

پژوهشنامه جغرافیای انتظامی سال هفتم، شماره بیست و هشتم، زمستان 1398
تاریخ دریافت: 1398/09/01 تاریخ پذیرش: 1398/12/10
از صفحه 115 تا 142

**چکیده**

در اثر توسعه روزافزون فناوری‌های مرتبط با فضای مجازی و استفاده از اینترنت، نوع و روش ارتکاب بسیاری از جرائم نیز تغییر جهت داده‌اند. دراین‌بین مجرمان مالی بیشترین سوءاستفاده را از این ابزار برای رسیدن به اهداف خود دارند که موجب افزایش نرخ این‌گونه جرائم شده است. هدف از این پژوهش بررسی توزیع مکانی قربانیان جرمِ برداشتِ غیرمجاز از حساب‌های بانکی در مناطق (۲۲) گانه شهر تهران است. روش پژوهش توصیفی تحلیلی استفاده از سیستم اطلاعات جغرافیایی است. سیستم اطلاعات جغرافیایی به مأموران انتظامی کمک می‌کند تا مکان‌های بالقوه جرم را توسط تحلیل معیارهایی که در ظاهر ارتباط چندانی با یکدیگر ندارند، به‌صورت نقشه و به شکل طبقه‌بندی‌شدهٔ گرافیکی شناسایی کند. جامعهٔ آماری شامل (۳۰۰) پرونده قربانیان این جرم در سال (۱۳۹۵) می‌باشد. تجزیه‌وتحلیل داده‌ها در دو بخش آمار توصیفی و استنباطی با به‌کارگیری روش‌های آماری-گرافیکی انجام شد. یافته‌ها نشان داد که آزمون مرکز متوسط قربانیان برداشت غیرمجاز حساب بانکی در فضای مجازی در منطقه (۶) قرار دارد. نتایج نشان داد که بین مؤلفه‌های اقتصادی، آموزشی و جمعیت با جرم موردمطالعه رابطه وجود دارد.

**کلیدواژه‌ها:** توزیع مکانی، قربانی، برداشت غیرمجاز از حساب‌های بانکی، شهر تهران.

1- استادیار گروه جغرافیای دانشگاه علوم انتظامی امین، تهران، ایران، (نویسنده مسئول)، barani.vahid@yahoo.com.
۲- استادیار گروه جغرافیای دانشگاه علوم انتظامی امین، تهران، ایران.
3- دانشیار گروه جغرافیای دانشگاه علوم انتظامی امین، تهران، ایران.

## بیان مسئله

طبق معمول دغدغه‌های امنیتی برای هر کسب‌وکاری وجود دارد و اکثراً از پشتیبانی امنیتی مناسبی برخوردار می‌باشند، اما همیشه این نوع پشتیبانی امنیتی در هر کسب‌وکار، حضور فعالی ندارد. برای بسیاری از شرکت‌های خصوصی و افراد خاص که امنیت مالی برای آن‌ها اهمیت زیادی دارد؛ به‌ویژه جایی که تأثیر جرم اغلب در افزایش هزینه‌های کالا، خدمات و کاهش سود حاصله به‌وضوح خود را نمایان می‌سازد؛ نکته مهم اینجاست که با استفاده روزافزون از اینترنت و فناوری مرتبط، بسیاری از این جرائم، در حال تغییر جهت در نحوه استفاده از اینترنت یا بهره‌برداری از فناوری رایانه هستند. در بعضی موارد، سخت‌ترین دفاع امنیتی در برابر حملات سایبری و افزایش خسارت احتمالی را مدنظر قرار می‌دهند؛ بنابراین برای مبارزه با این نوع جرائم، امنیت و اجرای قانون نیاز به ابزار متنوع، داشتن مهارت در نظارت و بررسی جرائم با استفاده از رایانه و فناوری اطلاعات ضروری به نظر می‌رسد (رابرت و همکاران[1]، ۲۰۱۹: ۴۸۷).

بر اساس آمار دادگستری ایالات‌متحده آمریکا، حدود (۷) درصد از ساکنان ایالات‌متحده آمریکا، مورد سرقت هویت در سال (۲۰۱۲) قرار گرفته‌اند؛ علاوه بر این، اطلاعات شخصی به سرقت رفته؛ برای ایجاد حساب بانکی، پیدا کردن یک شغل یا دریافت خدمات پزشکی مورداستفاده قرار گرفته است. برای مثال، با استفاده از اطلاعات شخصی قربانی، از جمله نام، آدرس و شماره صادرشده توسط دولت، به یک فرم شناسایی تبدیل‌شده و با استفاده از مدارک شناسایی جعلی به فرآیندهای ایجاد حساب‌های مالی کاذب و تسهیل دریافت خدمات منجر شده است (پیک و نالا[2]، ۲۰۱۵: ۶۲۷).

از جمله شهرهایی که میزان جرائم آن قابل‌توجه بوده و به دلیل مرکزیت کشوری و ویژگی الگو بودن آن نیاز به توجه بیشتری در این زمینه دارد، کلان‌شهر تهران است. تحلیل فضا و جغرافیای کلان‌شهر، ابزاری فنی محسوب می‌شود که اجازه می‌دهد تا شناخت زنده‌تر و بامعناتری از یک شهر و ساکنان آن داشته باشیم. ازاین‌روی ویژگی کلان‌شهر تهران ابزاری برای درک بیشتر تهران، ساکنان و سطح جرائم آن محسوب می‌شود (ذوالفقاری و شایگان، ۱۳۹۰: ۳). در این پژوهش سعی شده با استفاده از

1- Robert & atl
2- Peak & Nalla

ویژگی‌های جمعیتی، اقتصادی شهر تهران به چگونگی توزیع مکانی قربانیان جرم برداشت غیرمجاز از حساب‌های بانکی در شهر تهران پرداخته شود.

**جدول شماره (۱). خلاصهٔ پیشینه پژوهش.**

| پژوهشگران | نتایج |
|---|---|
| جاناتان جی راش (۱۳۷۹) | سه هدف مهم را دنبال کرد. نخست، تشخیص مهم‌ترین انواع کلاهبرداری‌های اینترنتی که مجریان قانون و قانون‌گذاران به آن‌ها برخورده‌اند؛ دوم، تشریح فنون عمده نفوذ روانی مورداستفاده مجرمان در این‌گونه کلاهبرداری‌ها و سوم، ارائه راهکارهایی برای این مسئله به دولت و بخش خصوصی. |
| وروایی و میرزکی (۱۳۹۰) | بخشی از شیوه‌های مقابله، نیازمند ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان‌ها در مورد مخاطرات سیستم‌های رایانه‌ای است، همچنین نظارت دائمی سازمان‌ها بر روی سامانه‌های رایانه‌ای و تدابیر امنیتی از قبیل حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت اطلاعات در مقابله با کلاهبرداری رایانه‌ای از اهمیت ویژه‌ای برخوردار است. |
| اسکندری‌پور و همکاران (۱۳۹۲) | بین میانگین مردان و زنان در رابطه با میزان آگاهی آنان از روش‌های جرائم تفاوت معنادار وجود ندارد. همچنین نتایج نشان داد که میزان تحصیلات بر روی میزان آگاهی آنان می‌افزاید. |
| وکیلی (۱۳۹۵) | تدوین قوانین مدون جهت پیشگیری از وقوع جرائم اینترنتی ضروری به نظر می‌رسد. |
| روضه‌ای و همکاران (۱۳۹۶) | از نظر خبرگان، آیتم‌های آموزش و آگاه‌سازی کاربران در خصوص کلاهبرداری اینترنتی، آموزش کاربران در خصوص خدمات بانکداری الکترونیکی توسط بانک‌ها و استفاده از نرم‌افزارهای امنیتی و ضدجاسوس‌افزارها توسط کاربران بیشترین تأثیر را در کاهش کلاهبرداری اینترنتی داشته‌اند؛ اما نتایج به‌دست‌آمده از سوی قربانیان جرم کلاهبرداری اینترنتی نشان می‌دهد که بیشترین تأثیر از بین عوامل به اولویت اول انجام احراز هویت و پروسه‌های تصدیق هویت؛ اولویت دوم افزایش سطح آگاهی و آموزش کاربران؛ و اولویت سوم استفاده از ابزارهای امنیتی متعلق می‌باشد. |
| توان‌بخش، دوستار و قیاسی (۱۳۹۶) | بین استانداردسازی بسترهای بانکداری الکترونیک و پیشگیری از فعالیت فیشینگ ارتباط معنی‌داری وجود دارد و همچنین، عدم آگاهی کاربران در خصوص فعالیت فیشینگ باعث ساده‌تر شدن کار فیشرها شده است. |
| کانشینگ[1] (۱۹۹۵) | با رشد روزافزون استفاده از اینترنت، ردیابی مجرمان برای پلیس بسیار دشوار شده است. |
| بیکر (۲۰۰۲) | بسیاری از شرکت‌های اینترنتی در طول سال‌های (۱۹۹۸) و (۱۹۹۹) با هویت پنهان مشغول فعالیت‌های فریبکارانه بودند که منجر به کلاهبرداری شد. باید |

1- Kaneshige

| پژوهشگران | نتایج |
|---|---|
| | اقداماتی برای کاهش اثرات منفی انجام گیرد. |
| سیمپسون[1] (۲۰۰۳) | اغلب کلاهبرداری‌ها، از طریق ایمیل یا خرید آنلاین و بانکداری بی‌حفاظ، آسان‌تر انجام می‌شود. گروه ePrivacy استاندارد امضاء دیجیتالی ایمیل و «اظهارات» درباره قصد و نیت فرستنده را به‌عنوان ابزاری پیشنهادی برای مبارزه با هرزنامه منتشر کرده است. |
| هالام بیکر[2] (۲۰۰۵) | حملات فیشینگ و فارمینگ به‌طور فزاینده‌ای پیچیده شده‌اند و این حملات از مهندسی اجتماعی تا مهندسی نرم‌افزار تکامل‌یافته است. آنان پیشنهاد دادند که مدیران فناوری اطلاعات، فروشندگان اینترنت و ارائه‌دهنده خدمات نرم‌افزاری باید اقدامات کوتاه‌مدت تاکتیکی را برای اقدام فوری انجام دهند. |
| اوریولا[3] (۲۰۰۵) | جامعه بین‌المللی به مقابله با کلاهبرداری نیجریه‌ای کمک کند و باعث شفافیت سامانمند، آمادگی اجرای قانون و تشدید کمپین‌های روشنگری عمومی و رویکردهای فناورانه برای مقابله با پیش‌زمینه تهدید کلاهبرداری در اینترنت شود. |
| ریموندچاو[4] (۲۰۱۱) | با توجه به تمایل مجرمان مالی برای دستیابی به اطلاعات شخصی و محرمانه، به طبع آن تنوع جرائم فضای مجازی افزایش‌یافته و حجم حملات نیز اجتناب‌ناپذیر شده است. همچنین تئوری فعالیت‌های روتین را برای کاهش خطرات با کاهش فرصت‌های جرم و جرائم فضای مجازی، ارائه دادند. |
| آلیم و آنتوی باوسیکو[5] (۲۰۱۱) | مشکل اساسی مقابله با کلاهبرداری در «eBay» ناتوانی ساختار پیشگیری از کلاهبرداری «eBay» در شناسایی و از بین بردن معامله گران کلاهبردار با هویت گمنام است. |
| جیمیسون و همکاران[6] (۲۰۱۲) | باید قانون فعلی در مورد کلاهبرداری هویتی تقویت شود و اقدامات پیشگیرانه برای جلوگیری از جرائم هویتی انجام شود. همچنین باید قوانین مربوط به جرائم هویتی جدید ایجاد شود. |
| ماسکون و همکاران[7] (۲۰۱۳) | امنیت فضای مجازی نقش مهمی در تضمین و محافظت از افرادی که از اینترنت در زندگی روزمره خود استفاده می‌کنند، دارد. همچنین سوءاستفاده از اینترنت مسئله‌ای جاری است که در برخی از موارد می‌تواند در یک دانشگاه اتفاق بیافتد. |
| اراچالج و لاو[8] (۲۰۱۴) | اثر متقابل دانش نظام‌مند و روان‌شناختی بر عملکرد کاربران رایانه تأثیر می‌گذارد. خودکارآمدی، باعث افزایش رفتارهای جلوگیری از تهدید فیشینگ می‌شود. همچنین آموزش مناسب بر پایه امنیت به کاربران کمک می‌کند، تهدیدات |

1- Simpson
2- Hallam-Baker
3- Oriola
4- Raymond Choo
5- Aleem & Antwi-Boasiako
6- Jamieson&et al
7- Maskun&et al
8- Arachchilage & Love

| پژوهشگران | نتایج |
|---|---|
| | فیشینگ را خنثی کنند. |
| وحدتی و یاسینی[1] (۲۰۱۵) | فضای سایبری به‌عنوان یک ابزار منحصربه‌فرد و مهم، اگر به‌خوبی مورداستفاده قرار نگیرند، این نوع جرائم کلاهبرداری که قبلاً شکل‌گرفته و یا هنوز شکل نگرفته‌اند، همچنان به‌طور نامناسب مورداستفاده قرار خواهند گرفت. |
| یوپ پیک و نالا[2] (۲۰۱۵) | سطح آموزش، فعالیت‌های روزمره آنلاین و ترس از سرقت هویت قربانی، با سرقت هویت قربانی رابطه مثبت دارد. |
| چاودری[3] (۲۰۱۶) | سارقان دیجیتال به طرز غیرمشکوک، کاربران اینترنتی را به‌عنوان طعمه‌های دیجیتال مورد هدف خود قرار می‌دادند تا سود حاصل از انواع برنامه‌های مخرب را به‌دست آورند. سرقت دسترسی به رایانه‌ها و محتوای دیجیتالشان به‌منظور بازخرید آن‌ها به مصرف‌کنندگان یا سازمان‌ها یکی از تهدیدهای پیشرو در زمینهٔ جرائم اینترنتی محسوب می‌شوند. |
| الرود و ژاو[4] (۲۰۱۷) | طبقه‌بندی قبلی فیشینگ، بیشتر تحت مکانیسم‌های فیشینگ تمرکز داشت؛ اما ظهور تکنیک‌های حمله سایبری، محیط‌های هدفمند را نشانه می‌گرفت و اقدامات مقابله با آن حملات خنثی می‌شد. آن‌ها یک طبقه‌بندی جدید شامل تکنیک‌های حمله، مقابله با اقدامات، محیط‌های هدفمند و رسانه‌های ارتباطی را پیشنهاد کردند. |

## مبانی نظری پژوهش

### عناصر تشکیل‌دهنده جرم کلاهبرداری و فریب در فضای مجازی

در قلمرو فضای مجازی، جایی که قوانین و مقررات چندانی وجود دارد، منظور از ارتکاب اقدام کلاهبرداری یا فریبکاری چیست؟ کسانی که اعمال فریبکارانه انجام می‌دهند، فقط به‌عنوان یک متخلف مجازات می‌شوند یا باید آن‌ها را به‌عنوان مجرم مجازات کرد؟ میچل و همکاران (۱۹۹۸) استدلال می‌کنند کلاهبرداری یک جرم است، جرم یقه‌سفید. آن‌ها بیان کردند جرمی یقه‌سفید است که:

به سوءاستفاده از موقعیت، قدرت، قاچاق موادمخدر، تجارت پنهانی، کلاهبرداری، دستمزد کم، نقض قوانین، سرقت، استثمار و اخفا که منجر به آسیب مالی، جسمی و روحی برخی افراد و اختلال در نهادها و اعتبارات اقتصادی، سیاسی و اجتماعی شود،

1- Vahdati & Yasini
2- Yeop Paek & Nalla
3- Chaudhry
4- Aleroud&Zhou

اشاره کند. میچل و همکاران (۱۹۹۸) استدلال می‌کنند که سطح جرم یقه‌سفید به‌عنوان سرمایه‌داری مالی افزایش‌یافته است و سیاست‌های اقتصادی لیبرال به فلسفه اقتصادی سیاسی سلطه‌گر تبدیل‌شده و این احتمال را بیشتر می‌کند که فعالیت‌های کلاهبرداری و جنایی، بدون مجازات و بدون پیشگیری حرکت کنند. به هر دلیلی، مقرراتی در اینترنت وجود دارد که اجازه می‌دهد میزان بروز اقدامات جنایی و فریبکاری کاهش یابد. میچل و همکارانش این مقاومت در برابر مقررات را بدین شرح توصیف می‌کنند: تلاش‌هایی برای تنظیم فعالیت اقتصادی ممکن است برای کسانی که «منافع خصوصی» یا «آزادی» خود را در معرض خطر می‌بینند و در معرض چنین مقرراتی قرار می‌گیرند، مقاومت می‌کنند. آن‌ها تلاش می‌کنند تا فشارهای فردی و جمعی را بر دولت تحمیل تا محدودیت‌های خود را کاهش دهند. در هنگام حمله به این مقررات، بخش کسب‌وکار به‌طور مرتب قوانینی را مطرح می‌کند و آن‌ها را به چالش می‌کشد. چراکه آن‌ها فعالیت اقتصادی را هدف قرار می‌دهند و از حق خود برای حفظ حریم خصوصی محروم می‌شوند. مقررات محرمانهٔ بعدی ممکن است بخش‌های بزرگی از کسب‌وکار را شامل شوند، اما علاوه بر ریسک از دست دادن حمایت عده‌ای برای آزادسازی، نتیجه آن در درازمدت ممکن است باعث تضعیف اعتماد شود، درحالی‌که اثرات فلج‌کنندهٔ نامعلوم، بیش از هزینه‌های موردقبول است (بیکر[1]، ۲۰۰۲: ۴).

**انواع مختلف از کلاهبرداری اینترنتی رایج در جهان**

- **کلاهبرداری به روش پیش‌پرداخت[2]**

هزینه‌های کلاهبرداری پیش‌پرداخت که از قربانیان می‌خواهند قبل از دریافت مقدار قابل‌توجهی از پول یا کالا، مبالغ قابل‌توجهی را پرداخت کنند. هزینه‌ها طبق معمول به‌عنوان مالیات، هزینه پردازش یا عوارض محضر صورت می‌گیرد. قربانی این هزینه‌ها را پرداخت می‌کند و در عوض چیزی دریافت نمی‌کند.

1- Baker
2- Advance Fee Frauds Schemes

- **کلاهبرداری کسب‌وکار یا استخدام**

به‌طورمعمول سرقت هویت، ارسال هزینه بار و طرح‌هایی از نوع چک تقلبی را شامل می‌شود. کلاهبردار یک سایت تبلیغاتی «شغل اینترنتی» را در اختیار شما قرار می‌دهد. متقاضیان این شغل با پر کردن برگه‌های اینترنتی، اطلاعات شخصی حساس، مانند تاریخ تولد و شماره امنیت اجتماعی خود را افشا می‌کنند. کلاهبردار این اطلاعات را برای خرید کالا از اعتبار شما استفاده می‌کند.

- **کلاهبرداری از کارت اعتباری**

کلاهبرداری از کارت‌های اعتباری، استفاده غیرمجاز از کارت اعتباری که به‌صورت نقدی و یا اموال به‌دست می‌آورند. شماره کارت‌ها اعتباری را می‌توان از وب‌سایت‌های غیرقانونی ربود و یا می‌تواند از طریق سرقت هویت شما به‌دست آورد.

- **کلاهبرداری از هویت افراد**

سرقت هویت زمانی رخ می‌دهد که فردی اطلاعات شخصی دیگری را بدون آگاهی از طریق سرقت و یا کلاهبرداری از اختیار دیگران بگیرد (آلیم و آنتوی باوسیکو، ۲۰۱۱: ۱۴۱).

- **هرزنامه؛ کلاهبرداری نیجریه‌ای**

ترفندهای قرعه‌کشی، نوع جدیدی از کلاهبرداری‌های ایمیلی هستند که به‌طور عمده در آفریقای غربی آشکار می‌شوند و دارای برچسب «خیلی محرمانه» یا «بسیار فوری» هستند. فرستنده پسر یا دختر یک حاکم عزل شده درجایی در غرب آفریقا یا آفریقا مرکزی یا یکی از بستگان قربانیان جنگ‌های داخلی چندساله آفریقا یا یک مدیر ارشد مالی مؤسسهٔ مالی نیجر است.

چند میلیون دلار ایالات‌متحده آمریکا در یک مؤسسهٔ مالی در نیجریه، ساحل‌عاج، زیمبابوه، آفریقای جنوبی یا آنگولا قرار دارد. این پول متعلق به یک مشتری فوت‌شده خارج از مؤسسهٔ مالی با هیچ نسبت فامیلی قابل‌ردیابی نیست و یا متعلق به یک حاکم فوت‌شده یا متعلق به یک قربانی سیاست زراعت توزیع زمین زراعی در زیمبابوه و غیره نیست. همدست شما به‌شدت به دنبال یافتن این پول از خارج از آفریقا در یک حساب خارجی (خود) است. فرستنده خواستار ارسال شماره‌حساب بانکی، شماره پین، تلفن،

دورنگار و غیره از شما است. اگر پاسخ شما مثبت بود، فرستنده پس‌ازآن به‌صورت سامانمند پول شما را برداشت می‌کند که طبق معمول از طریق شرکت مالی «وسترن یونیون[1]» منتقل خواهد کرد. ظاهراً این پول برخی از «هزینه‌های رسمی» یا «هزینه وکالت» را پوشش می‌دهد. اگر واقعاً فرد بی‌تجربه باشد، فرستنده به‌سرعت حساب فرد قربانی را قبل از اینکه بداند فریب‌خورده است، خالی می‌کند. افرادی که دارای ملیت‌های گوناگون‌اند، قربانیان این نوع کلاهبرداری هستند؛ درحالی‌که برخی از قربانیان هدف، ایمیل کلاهبرداری را به پلیس نیجریه فرستاده‌اند. درحالی‌که بسیاری از قربانیان، گزارش‌های خود را به مقامات کشورشان ارائه می‌دهند، برخی قربانیان از شرم این نوع کلاهبرداری، نمی‌خواهند گزارشی را به مقامات ارائه دهند؛ بنابراین حساب کاربری نیجریه نوعی از کلاهبرداری اینترنتی است که به‌عنوان «کلاهبرداری پیش‌پرداخت» شناخته‌شده است، یا با اختصار نامناسب آن: خطای (۴۱۹). بخشی تحت قانون جزایی در نیجریه هست که منجر به کسب اموال با اظهارات دروغین می‌شود. این جرائم به‌طور سنتی توسط دورنگار، تلفن و پست قبل از ظهور اینترنت مورداستفاده قرارگرفته است. بااین‌حال، در فضای اینترنت، این نوع جرائم به‌صورت جسورانه به ایمیل‌های کلاهبرداری تغییر و در همه‌جا گسترش یافت (اوریولا، ۲۰۰۵: ۲۳۹).

**جغرافیای فضای مجازی**

ادراک فضا، تلاش برای فهم کنش انسانی در محیط است. حال‌آنکه محیط تنها دربرگیرنده زمین نخواهد بود؛ زیرا چشم‌انداز مکانی داشتن از فضا، محدودکنندهٔ تحلیل‌های فضائی به‌خصوص در عصر ارتباطات است.

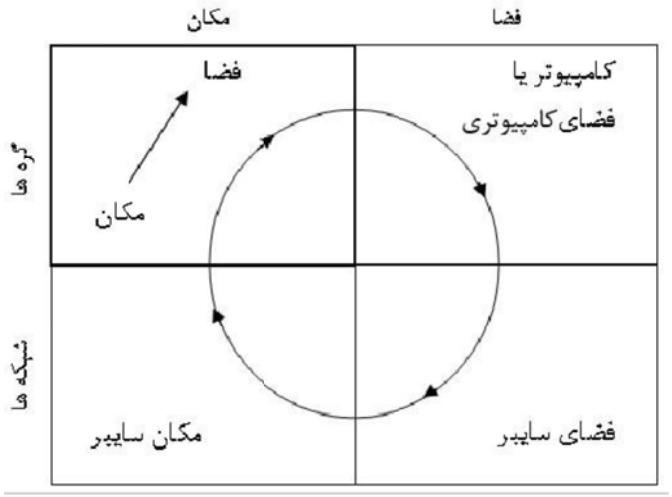
فرآیند فضائی، سازوکاری است که ساخت فضایی یک یا چند پدیده را به وجود می‌آورد. هر فرآیند فضایی، بیشتر حاصل تصمیمات انسانی است.

ازاین‌رو، می‌توان در تحلیل فضای فناورانه نقشی برای تصمیمات انسانی قائل بود. درواقع فضای مجازی این امکان را می‌دهد تا افراد و سازمان‌ها به شکلی انعطاف‌پذیرتر در ارتباط با فضای جغرافیایی واقعی عمل نمایند. کارکردهای واقعیت و مجازیت در حال تبدیل‌شدن به دو جبهه مخالف یکدیگر هستند؛ زیرا برخی از مخالفان فضای مجازی از

1- Western Union

توسعهٔ این فضا و اشراف آن بر فضای واقعی بیم دارند. آنان تزلزل و چندوجهی عمل نمودن فضای مجازی را عاملی برای تحریف حقایق عنوان می‌کنند؛ بنابراین پیش‌بینی می‌شود این مخالفت‌ها همچنان، به‌خصوص با فراگیرتر شدن فضای مجازی ادامه یابد. تحولاتی که در جهان می‌گذرد از دیدگاه واقعی، حاصل فرآیندهای طبیعی است و این موضوع در فضای مجازی حاصل داده‌های اطلاعاتی است.

این حقیقتی است که واقعیت مجازی باعث درهم آمیختن محیط طبیعی و محیط مجازی شده است؛ بنابراین شالوده‌های درهم‌تنیده واقعیت و مجاز در عصر ارتباطات امکان انحصارگرایی آنان را میسر نمی‌سازد، بلکه به نظر می‌رسد مجازیت در آینده بر واقعیت مشرف و واقعیت در حکم تأمین‌کننده اطلاعاتی فضای مجازی گام بر خواهد داشت.




**شکل شماره (۱). الگوی مفهومی فضا، مکان، فضای سایبری (شکویی ۱۳۸۲).**

تبیین شکل شماره (۱) و فرآیندهای موجود در آن می‌تواند جغرافیای سایبر را بهتر متصور سازد. مکان و فضای موجود در فضای سایبر دربردارنده رایانه‌های بسیار و نیز فضای رایانه‌ای شامل برنامه‌ها، نرم‌افزارها، اطلاعات و ماشین‌آلات شخصی است که آن‌ها در محیطی به‌واسطه نودها و شبکه‌ها به یکدیگر پیوند خورده می‌شود و چشم‌انداز جغرافیای سایبر را به وجود می‌آورند (شکوئی، ۱۳۸۲: ۹۰).

**حقه زدن ایمیلی «پی پال[1]» از مظنون در کلاهبرداری «eBay» در مکان‌های مختلف جغرافیایی**

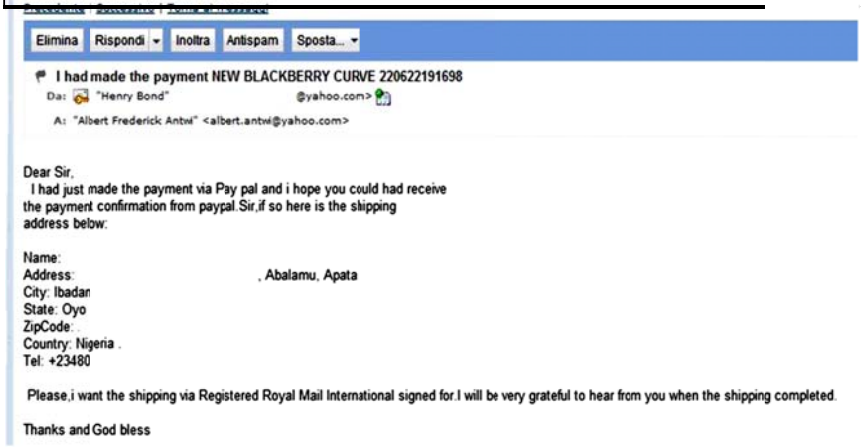
این فعالیت فریبنده فقط پس از تائید پرداخت در «پی بال» جعلی کشف شده بود. تجزیه‌وتحلیل قانونی از ایمیل تأیید پرداخت «پی بال» جعلی و سایر ایمیل‌های دیگر از هنری باند، همان آدرس IP را نشان داد که نباید مورد تأیید قرار گیرد؛ زیرا ایمیل‌های «پی بال» از شهر ایبادان ساخته نمی‌شوند. دو مظنون دیگر با همان آدرس IP به‌عنوان هنری باند آدرس[2] متفاوت ارائه دادند.

**جدول شماره (۲). تجزیه‌وتحلیل ایمیل تأیید پرداخت «پی بال» جعلی و سایر ایمیل‌های دیگر از هنری باند.**

| Path | IP | Hostname | Country | City | Latitude | Longitude | ISP |
|---|---|---|---|---|---|---|---|
| Sender | 41.184.112.100 | Unknown | Nigeria | Ibadan | 7.3878 | 3.8964 | AS29091 ipNX Nigeria Limited |
| Path Point | 64.12.224.143 | web-mmc-m10.sim.aol.com | United States | N/A | 38 | -97 | AS1668 |
| Path Point | 205.188.170.2 | smtprly-dc02.mx.aol.com | United States | N/A | 38 | -97 | AS1668 |
| Path Point | 64.12.78.137 | imo-ma02.mx.aol.com | United States | N/A | 38 | -97 | AS1668 |
| Path Point | 127.0.0.1 | Local network computer | | | | | |
| Destination | 205.188.91.95 | imr-db01.mx.aol.com | United States | N/A | 38 | -97 | AS1668 |

جدول ردیابی نشان‌دهنده آدرس IP که مظنون به کلاهبرداری eBay می‌باشد.

1- PayPal
2- delivery address



Elimina | Rispondi | Inoltra | Antispam | Sposta...

I had made the payment NEW BLACKBERRY CURVE 220622191698

Da: "Henry Bond" @yahoo.com>

A: "Albert Frederick Antwi" <albert.antwi@yahoo.com>

Dear Sir,
I had just made the payment via Pay pal and i hope you could had receive the payment confirmation from paypal.Sir,if so here is the shipping address below:

Name:
Address: , Abalamu, Apata
City: Ibadan
State: Oyo
ZipCode:
Country: Nigeria .
Tel: +23480

Please,i want the shipping via Registered Royal Mail International signed for.I will be very grateful to hear from you when the shipping completed.

Thanks and God bless

**شکل شماره (۲). ایمیل فرستاده‌شده توسط هنری باند به همراه آدرس ارسالی.**

واقعیت این است که تمام ایمیل‌های مشتمل بر سه مظنون مختلف از همان آدرس IP منشأ گرفته‌شده و تمام پنج مظنون از کشور نیجریه یک تاکتیک فریبنده را به‌کاربرده‌اند و حداقل یکی از این نگرانی‌ها را برجسته کرده‌اند:

۱- دخالت شبکه جنایی سازمان‌یافته؛

۲- احتمال این‌که یک معامله‌گر، چندین حساب «eBay» را اداره می‌کند.

هنری باند، مظنونی که در همه ابعاد، ظهور این سوءاستفاده فریبکارانه جدید را نشان داد، ایمیل (شکل شماره ۱) فرستاده‌شده توسط اداره رسیدگی به شکایات اینترنت مرکز فدرال از طریق «پی بال» ارسال‌شده بود. این ایمیل پس‌ازاینکه مظنون، اقدامات جعلی را برای محققین و تحویل «بلک‌بری» انجام داد، ارسال شده بود. یک‌بار دیگر، تجزیه‌وتحلیل قانونی این ایمیل فرستاده‌شده، نشان داد که ایمیل توسط هنری باند از کشور نیجریه ارسال شده است نه از پایگاه FBI در شهر نیویورک. به‌احتمال‌زیاد افرادی که از کلاهبرداری در «eBay» آگاهی دارند، می‌توانند این ترفندهای فریبنده را شناسایی کنند؛ بااین‌حال، سناریوی بالا، قابلیت‌های فنی پیچیدهٔ کلاهبرداری را به‌منظور بهره‌برداری از فرصت‌ها و مکانیسم‌های مختلف برای انجام کلاهبرداری در مناطق مختلف جهان، مشخص می‌کند (آلیم و آنتوی باوسیکو، ۲۰۱۱: ۱۵۱).

**جرم‌ها در فضاهای جغرافیایی**

نرخ حوادث جنایی در تمام کشورهای توسعه‌یافته به علت تغییر حالت زندگی و شرایط محیطی در حال افزایش است. جرائم به‌طور خودبه‌خود پدیدار نمی‌شوند و اداره پلیس وظیفهٔ دفاع و حفظ امنیت و سلامتی افراد جامعه را بر عهده دارد؛ بنابراین بایستی فعالیت‌های پلیس برای شناسایی موقعیت‌ها و تعیین زمانی که بیشترین فعالیت‌های مجرمانه رخ می‌دهد، تداوم یابد. برای کاهش و رفع جرائم، بعضی از فعالیت‌ها نظیر جلوگیری از وقوع جرم بایستی انجام شود. سیستم اطلاعات جغرافیایی[1] به مأموران انتظامی کمک می‌کند تا مکان‌های بالقوه جرم را توسط تحلیل معیارهایی که در ظاهر ارتباط چندانی با یکدیگر ندارند، به‌صورت نقشه و به شکل طبقه‌بندی‌شده گرافیکی شناسایی کنند. امروزه GIS بیشترین استفاده در پیش‌بینی جرم را یافته است و در نتیجه مناطق جغرافیایی خاص را مورد هدف منابع پلیس قرار می‌دهد و این کاربردها شامل تحقیقات قانونی محیطی نظیر زباله‌های صنعتی و بازرسی آگاهانه از صحنه‌های جرم می‌باشد. افزون بر این GIS به‌عنوان ابزاری برای کمک به نیروهای پلیس به‌منظور طراحی مؤثر پاسخ‌های ضروری، تعیین اولویت‌های تجزیه‌وتحلیل حوادث تاریخی و پیش‌بینی حوادث در آینده استفاده می‌شود (اکبری و همکاران، ۱۳۹۲: ۶۷).

ابزارهای زیادی برای تحلیل و نمایش مجموعه داده‌های مربوط به جرائم وجود دارد؛ اما نرم‌افزارهای GIS با توجه به قابلیت‌هایی که دارند، می‌توانند یک خروجی دیداری تولید کنند که ترکیبی از مجموعه داده‌های مختلف را دریک خروجی معنی‌دار ارائه نمایند. با کمک قابلیت به هنگام GIS می‌توان جرائم حادث‌شده در منطقه شهری را وارد نقشه‌های مکانی شهری کرد و مناطق امن و پرخطر از لحاظ میزان جرم و جنایت را شناسایی و تدابیر امنیتی-انتظامی لازم را اتخاذ کرد (قربانی سپهر، ۱۳۹۷: ۷).

ازآنجاکه جرم‌ها در فضاهای جغرافیایی رخ می‌دهند و مأموران پلیس وقتی‌که داده‌های فضایی را به‌صورت گرافیکی نمایش می‌دهند، بهتر می‌فهمند؛ بهترین راه نمایش آن‌ها استفاده از نقشه است. افسران اجرای قانون با داشتن نقشه بهتر می‌توانند تحلیل کنند که چرا یک نمونه جرم در یک منطقه خاص بیشتر اتفاق می‌افتد (قربانی

1- GIS

شپهر، ۱۳۹۲: ۷-۸). مکان‌های جرم‌خیز و ویژگی‌های متفاوتی که هریک از این مکان‌ها دارند، اصطلاحات فرعی دیگری نیز در ارتباط با کانون‌های جرم‌خیز ارائه داده‌اند که عبارت‌اند از:

۱- نقاط جرم‌خیز یا نقاط داغ[1]:

به محدوده‌های مشخص و با ابعادی کوچک‌تر از مکان‌های جرم‌خیز اطلاق می‌شود. در واقع این واژه به تمرکز جرم در برخی مکان‌های شهری اشاره دارد و نشان‌دهنده آن است که در برخی نقاط مشخص به‌دفعات عمل مجرمانه تکرار می‌شود.

۲- مسیرهای جرم‌خیز یا مسیرهای داغ[2]:

به محدوده‌های وسیع‌تر از نقاط جرم‌خیز گفته می‌شود و دلالت بر تمرکز بزهکاری در طول یک خیابان یا مسیر عبوری دارد.

۳- نواحی جرم‌خیز یا نواحی داغ[3]:

منظور تمرکز بزهکاری درون یک محدوده جغرافیایی شامل یک ناحیه یا بخش یا محله شهری است که وسعتی به‌مراتب بیشتر از نقاط و مسیرهای جرم‌خیز دارد.

۴- اموال یا اشیاء در معرض بزهکاری مکرر[4]:

به برخی کالاها یا اموالی اطلاق می‌شود که مطلوب بزهکاران بوده و برای آنان جذابیت فراوان دارد و طبق معمول این اموال یا اشیا به‌طور مستمر هدف اعمال مجرمانه آن‌ها قرار می‌گیرد. به‌عنوان‌مثال تلفن همراه یا ضبط خودرو از جمله این‌هاست.

۵- مردم در معرض بزهکاری مداوم[5]:

به شهروندانی اطلاق می‌شود که به‌کرات در معرض اقدامات مجرمانه قرار می‌گیرند (کلانتری و توکلی، ۱۳۸۶: ۷۸-۷۹).

---

1- Hot spot
2- Hot routes
3- Hot dots
4- Hot areas
5- Hot peoples

## روش پژوهش

روش پژوهش حاضر تحلیلی-تطبیقی است. اطلاعات موردنیاز از میزان و نوع جرم به‌صورت کتابخانه‌ای از نیروی انتظامی اخذشده و برای شناسایی و درک الگوهای مکانی کلاهبرداری در فضای مجازی در شهر تهران از مدل‌های آماری و گرافیک به‌عنوان مبنا استفاده‌شده است. جامعه آماری در این پژوهش (۳۰۰) پرونده شامل قربانیان برداشت غیرمجاز از حساب‌های بانکی در فضای مجازی در سال (۱۳۹۵) در مناطق (۲۲) گانه شهر تهران است. تجزیه‌وتحلیل داده‌ها در دو بخش آمار توصیفی و استنباطی انجام‌شده است. پیرامون تجزیه‌وتحلیل داده‌ها در این پژوهش در بخش آمار توصیفی و بررسی پرسش‌های جمعیت شناختی از تکنیک‌هایی نظیر میانگین، محاسبه فراوانی و درصد استفاده شده است. همچنین در تجزیه‌وتحلیل اطلاعات این پژوهش از روش‌های آماری-گرافیکی در قالب سیستم اطلاعات جغرافیایی بهره گرفته‌شده است. مهم‌ترین آزمون‌های مورداستفاده در این پژوهش عبارت‌اند از:

**مرکز متوسط**[1]: مرکز متوسط را می‌توان به‌عنوان معیاری تقریبی برای مقایسهٔ توزیع فضایی انواع گوناگون جرم یا برای بررسی وقوع یک نوع جرم خاص در دوره‌های زمانی مختلف به کار گرفت. اندازه‌گیری جابجایی فضایی یک نوع جرم خاص از این جمله است. میانگین مرکزی به‌صورت رابطه شماره (۱) حساب می‌شود:

رابطه شماره (۱):

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n} \quad , \quad \bar{Y} = \frac{\sum_{i=1}^{n} Y_i}{n}$$

**بیضی انحراف معیار**[2]:

توزیع بسیاری از پدیده‌های جغرافیایی در فضا به‌گونه‌ای هستند که ممکن است جهت‌دار بوده و نتوان آن‌ها را با دایره نشان داد. در این موارد می‌توان با محاسبه واریانس محورهای X و Y به‌طور جداگانه و مستقل روند و جهت توزیع پدیده‌ها را در فضا نشان داد. آزمون بیضی انحراف معیار با استفاده از فرمول زیر به‌دست می‌آید:

1- Mean Center
2- Standard Deviation Ellipse

رابطه شماره (۲):

$$SDE_x=\sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n}} \quad و \quad SDE_y=\sqrt{\frac{\sum_{i=1}^{n}(y_i-\bar{y})^2}{n}}$$

در این رابطه $X_i$ مختصات عارضه $i$ بوده و $\{x,y\}$به ترتیب میانگین مرکزی عوارض $n$ برابر با تعداد کل عوارض در لایه مورد تحلیل است. زاویه چرخش نیز به‌صورت رابطه شماره (۴) محاسبه می‌شود:

رابطه شماره (۳):

$$\tan\theta=\frac{A+B}{C}$$
$$A=\left(\sum_{i=1}^{n}x_i^2-\sum_{i=1}^{n}y_i^2\right)$$
$$B=\sqrt{\left(\sum_{i=1}^{n}x_i^2-\sum_{i=1}^{n}y_i^2\right)^2+4\left(\sum_{i=1}^{n}x_iy_i\right)^2}$$
$$C=2\sum_{i=1}^{n}x_iy_i$$

در اینجا $X_i$ و $Y_i$ اختلاف بین مختصات $x$ و $y$ از میانگین مرکزی است. همچنین انحرافات استاندارد برای محورهای $x$ و $y$ چنانچه در رابطه شماره (۴) نشان داده‌شده است، عبارت‌اند از:

رابطه شماره (۴):

$$\sigma_x=\sqrt{\frac{\sum_{i=1}^{n}(\bar{x}_i\cos\theta-\bar{y}_i\sin\theta)^2}{n}}$$
$$\sigma_y=\sqrt{\frac{\sum_{i-1}^{n}(\bar{x}_i\sin\theta-\bar{y}_i\cos\theta)^2}{n}}$$

## یافته‌های پژوهش

### توزیع و درصد فراوانی جرائم بر اساس بازه زمانی

جدول **شماره** (۳) توزیع فراوانی و درصد فراوانی وقوع جرائم بر اساس بازه زمانی را نشان می‌دهد. همان‌طور که مشاهده می‌شود، بیشترین آمار وقوع جرائم مربوط به بازه

زمانی ۰۷۰۰- ۱۰۰۰، (۲۹/۳) درصد است که آمار مربوط به زمان جرائم به تفکیک در جدول **شماره** (۳) آمده است:

**جدول شماره (۳). محاسبه فراوانی و درصد وقوع جرم بر اساس بازه زمانی.**

| بازه زمانی | فراوانی | درصد |
|---|---|---|
| ۰۴۰۰-۰۱۰۰ | ۶ | ۲ |
| ۷۰۰ -۰۴۰۱ | ۱۸ | ۶ |
| ۱۰۰۰-۰۷۰۱ | ۸۸ | ۲۹/۳ |
| ۱۳۰۰-۱۰۰۱ | ۷۷ | ۲۵/۷ |
| ۱۶۰۰-۱۳۰۱ | ۵۶ | ۱۸/۷ |
| ۱۹۰۰-۱۶۰۱ | ۴۳ | ۱۴/۳ |
| ۲۲۰۰-۱۹۰۱ | ۱۲ | ۴ |
| جمع کل | ۳۰۰ | ۱۰۰ |

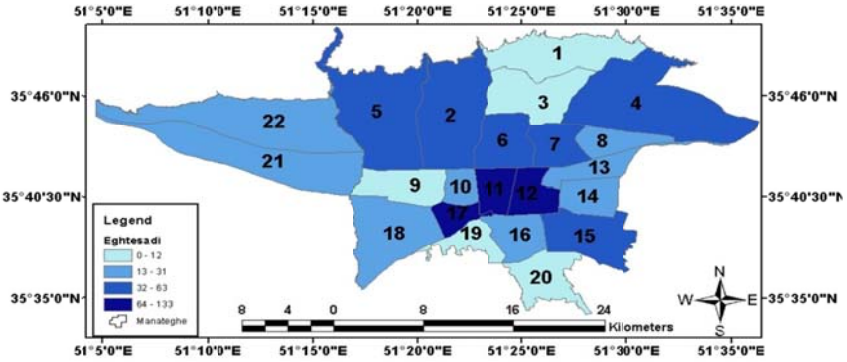
**توزیع مکانی قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان تهران در فضای مجازی در شهر تهران چگونه است؟**

**ویژگی‌های توصیفی-فضایی مناطق (۲۲) گانه شهرداری شهر تهران**

**توزیع فضایی فعالیت‌های اقتصادی شهر تهران**

یکی از مهم‌ترین شاخص‌هایی که با آن می‌توان به شناخت الگوی کار در یک فضای اقتصادی پرداخت، شاخص‌های توزیع فعالیت اقتصادی است. تمرکز بسیار بالای فعالیت‌ها و واحدهای تجاری در منطقه (۱۲) و همچنین نواحی هم‌مرز با منطقه (۱۲) یعنی نواحی مناطق (۶)، (۱۱)، (۱۶) و (۱۵) یک هسته فعالیت را در این محدوده با (۲۷۷۷۵) واحد فعالیتی شکل داده است. تعجبی ندارد اگر منطقه (۲۱) شهر تهران با انبوه کارخانه‌های بزرگ و گستره بزرگ صنعتی جزء کانون‌های نسبتاً کم تراکم قرارگرفته است. بزرگ‌ترین محدودهٔ اشتغال یا هسته اصلی اشتغال در شهر تهران جایی که بیشترین افراد شاغل محل فعالیتشان در آنجا قرارگرفته، با هسته اصلی کانون‌های فعالیت در شهر تهران انطباق دارد. منطقه (۲۱) تهران به دلیل تعداد بالای شاغلان به‌خصوص وجود واحدهای فعالیتی با بیش از (۱۰۰) نفر کارکن، ازلحاظ اشتغال در حد متوسط قرارگرفته است. این هسته یک هسته فعالیتی چند کارکردی است که در آن فعالیت‌های فرهنگی، اداری، تجاری و کارگاهی در حال انجام است. بزرگ‌ترین

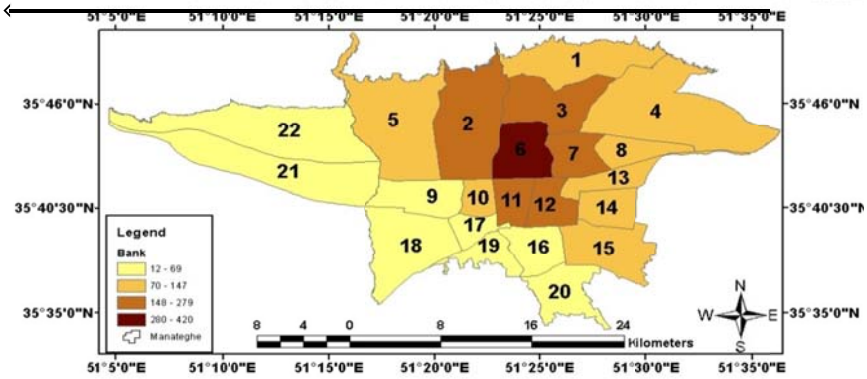
راسته‌های فعالیتی تهران در این هسته قرارگرفته و بیشترین سفرهای روزانه به‌قصد کار در این هسته انجام می‌پذیرد. تمرکز برخی فعالیت‌ها در خارج از هسته اصلی فعالیت‌ها، مشخص‌کننده کارکرد اصلی این مناطق در شهر تهران است (اطلس کلان‌شهر شهر تهران، ۱۳۸۵). به‌طورکلی ازنظر شاخص‌های اقتصادی، مناطق (۲)، (۴)، (۵)، (۶)، (۷)، (۱۷)، (۱۲)، (۱۱) و (۶) بالاترین سطح و در مقابل به ترتیب مناطق (۱۹)، (۳)، (۱) و (۲۰) پایین‌ترین سطح و رتبه را دارند.




**شکل شماره (۳). توزیع فضایی فعالیت‌های اقتصادی شهر تهران (منبع: یافته‌های پژوهش).**

### توزیع فضایی بانک‌ها و مؤسسات مالی شهر تهران

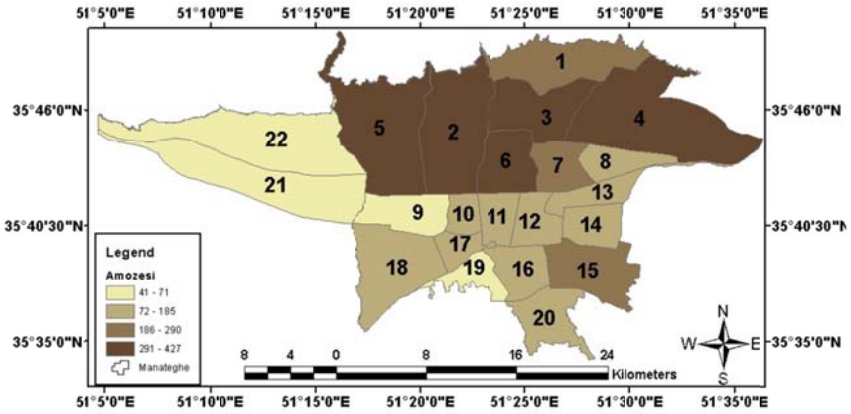
ازنظر توزیع فضایی بانک‌ها و مؤسسات مالی منطقه (۶) بیشترین تعداد بانک‌ها و مؤسسات مالی را به خود اختصاص داده و سپس مناطق پیرامونی آن شامل (۱۱)، (۷)، (۳)، (۲) و (۱۲) بالاترین تعداد مؤسسات مالی را در خود جای‌داده است. کمترین توزیع فضایی بانک‌ها و مؤسسات مالی را منطقه (۹)، (۲۱)، (۲۰)، (۱۹)، (۱۸)، (۱۷)، (۱۶) و (۲۲) به خود اختصاص داده‌اند.




**شکل شماره (۴). توزیع فضایی فعالیت‌های بانکی شهر تهران (منبع: یافته‌های پژوهش).**

### توزیع فضایی مراکز آموزشی شهر تهران

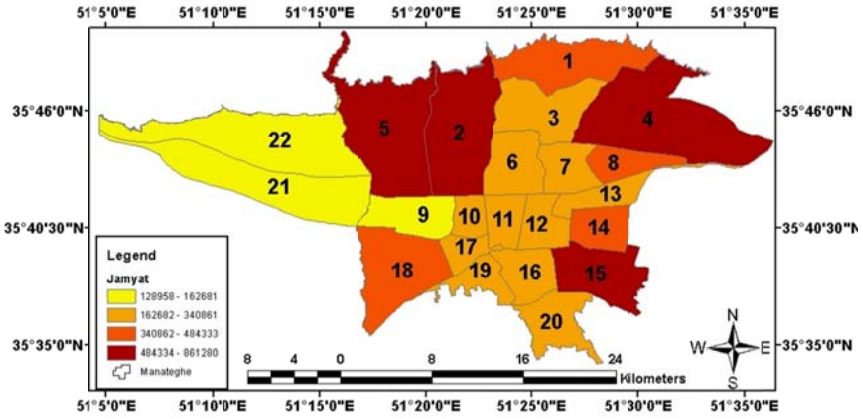
ازنظر توزیع فضایی مراکز آموزشی شهر تهران، یافته‌ها نشان می‌دهد مناطق (۶)، (۵)، (۴)، (۳) و (۲) بیشترین فضای مراکز آموزشی را به خود اختصاص داده است و کمترین توزیع فضایی مراکز آموزشی را مناطق (۲۱)، (۱۹)، (۹) و (۲۲) را به خود اختصاص داده است.




**شکل شماره (۵). توزیع فضایی مراکز آموزشی شهر تهران (منبع: یافته‌های پژوهش).**

### توزیع فضایی استقرار جمعیت شهر تهران

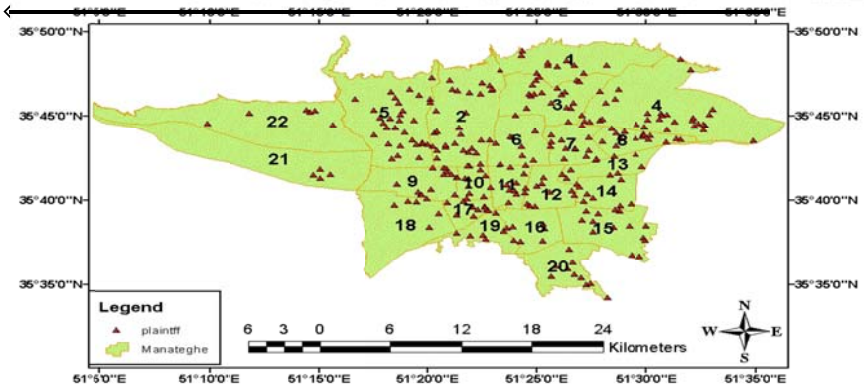
ازنظر توزیع فضایی استقرار جمعیت، مناطق (۱۵)، (۴)، (۲) و (۵) بیشترین استقرار جمعیت و بعدازآن مناطقی مانند (۱۸)، (۱۴) و (۱) را شامل شده است؛ اما کمترین توزیع فضایی استقرار جمعیت را مناطقی مثل (۲۱)، (۹) و (۲۲) به خود اختصاص داده است.




**شکل شماره (۶). توزیع فضایی استقرار جمعیت شهر تهران (منبع: یافته‌های پژوهش).**

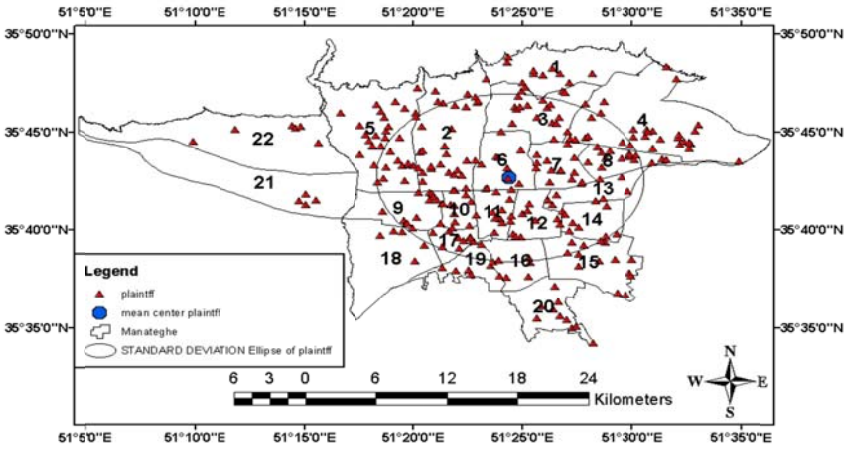
### تحلیل توزیع مکانی-فضایی قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان در فضای مجازی در مناطق (۲۲) گانه تهران

توزیع مکانی قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان تهران از طریق فضای مجازی، در مناطق (۲۲) گانه شهرداری تهران مشاهده شد. این نقشه نشان می‌دهد که بیشترین توزیع مکانی قربانیان جرائم برداشت غیرمجاز حساب بانکی به ترتیب در مناطق مرکزی و شمال شهر تهران و کمترین توزیع جرائم برداشت غیرمجاز حساب بانکی در مناطق غرب و جنوب غرب مشاهده‌شده است.



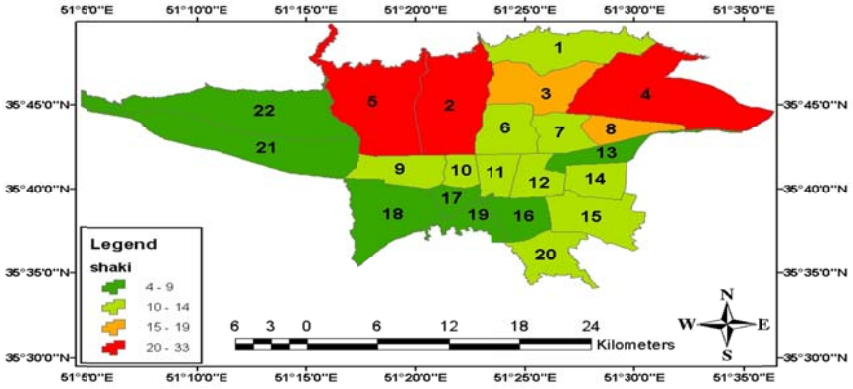

**شکل شماره (۷). توزیع مکانی قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان از طریق فضای مجازی در مناطق (۲۲) گانه شهرداری تهران.**

در شکل شماره (۸) مرکز متوسط بیضی انحراف قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان از طریق فضای مجازی در مناطق (۲۲) گانه شهرداری تهران مشاهده می‌شود. مرکز متوسط بیضی انحراف جرائم برداشت غیرمجاز حساب بانکی در منطقه (۶) شهرداری قرارگرفته است و بیضی انحراف معیار این نوع جرم در جهت شرقی –غربی در مرکز شهر تهران قرار دارد.



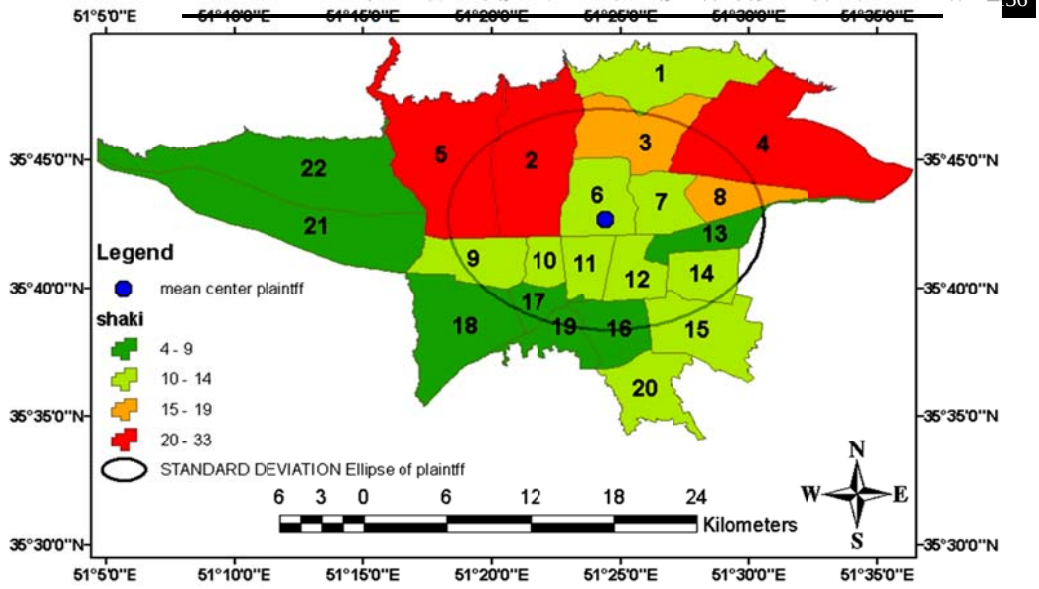

**شکل شماره (۸). مرکز متوسط و بیضی انحراف قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان از طریق فضای مجازی در مناطق (۲۲) گانه شهرداری تهران.**

در شکل شماره (۹) طبقه‌بندی قربانیان جرائم سایبری مالی در مناطق (۲۲) گانه شهرداری تهران مشاهده می‌شود. در این تصویر تعداد و توزیع قربانیان جرائم برداشت غیرمجاز حساب بانکی با استفاده از رنگ مشخص شده است. برابر شکل ارائه‌شده، بیشترین تعداد قربانیان جرائم برداشت غیرمجاز حساب بانکی در منطقه‌های (۵)، (۴) و (۲) و کمترین تعداد قربانیان در مناطق (۲۰)، (۱۹)، (۱۸)، (۱۷)، (۱۶) و (۲۱) مشاهده‌شده است.




**شکل شماره (۹). توزیع قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان از طریق فضای مجازی در مناطق (۲۲) گانه شهرداری تهران.**

در شکل شماره (۱۰) به‌وضوح تطابق بین توزیع و تعداد قربانیان جرائم و مرکز متوسط و بیضی انحراف قربانیان جرائم برداشت غیرمجاز حساب بانکی در مناطق (۲۲) گانه شهرداری تهران مشاهده می‌شود. مرکز متوسط بیضی انحراف قربانیان جرائم در این تصویر بین مناطق (۷) و (۶) در شرق و غرب که بیشترین تمرکز جرائم دیده می‌شود و نیز بین مناطق (۱۲)، (۱۴)، (۱۱)، (۱۰) و (۹) در قسمت جنوبی دیده می‌شود.




**شکل شماره (۱۰). تطابق مرکز متوسط و بیضی انحراف و طبقه‌بندی قربانیان جرم برداشت غیرمجاز حساب بانکی شهروندان از طریق فضای مجازی در مناطق (۲۲) گانه شهرداری تهران.**

## نتیجه‌گیری

ارتباط بین مرکز متوسط و بیضی انحراف استاندارد قربانیان با مؤلفه‌های موردمطالعه که به ترتیب، اقتصادی، بانک، آموزشی و جمعیت را نشان می‌دهد. در یافته‌های پژوهش نشان داده شد که آزمون مرکز متوسط قربانیان برداشت غیرمجاز حساب بانکی در فضای مجازی در منطقه (۶) قرارگرفته‌اند. نقاط مرکز متوسط رخداد کلاهبرداری در فضای مجازی درواقع در مرکز کانون‌هایی فعالیت‌های بانک، آموزشی و یا در پیرامون مناطقی که بیشترین فعالیت اقتصادی و تحرکات جمعیتی قرار دارند. بیضی انحراف استاندارد رخداد کلاهبرداری (قربانی) نیز با یک الگوی جهت‌دار یعنی جهت شرقی-غربی از بُعد فضایی، مناطق وسیعی از شهر تهران را تحت پوشش خود قرار داده است و مناطقی چون (۲۲)، (۲۰) و (۱) خارج بیضی انحراف استاندارد قرارگرفته‌اند. پیش‌بینی می‌شود که اگر این یافته‌ها در اختیار مؤسسات مالی و بانک‌ها و تاجران قرار گیرند، اقدام مؤثری در جهت اطلاع‌رسانی در این نوع جرم نکنند. این موضوع برمی‌گردد به

واقعیتی که مور در سال (۲۰۱۰) بیان کرد «بانک‌ها نمی‌خواهند فساد مالی ناشی از کلاهبرداری را با خطر ترساندن مشتریان، باعث دور کردن مشتریان از بانکداری آنلاین کنند. بازرگانان نمی‌خواهند با پلیس در مورد حوادث جاسوسی سایبری همکاری کنند؛ زیرا ممکن است به شهرت آن‌ها (و قیمت سهام آن‌ها) ضربه بزند؛ اپراتورهای زیرساخت حیاتی، نمی‌خواهند اطلاعات مربوط به قطع شدن ناشی از حملات مخرب را، با ترس جلوه دادن آسیب‌پذیری‌های سامانه‌ای، مشتریان را نگران کنند.» نتایج این تحقیقات انجام‌گرفته به‌نوعی به تأیید بخشی از پژوهش وحدتی و یاسینی (۲۰۱۵) است؛ یعنی به‌واسطه اینکه فضای مجازی به‌خوبی مورداستفاده قرار نگرفت این نوع جرائم دوباره به‌نوعی دیگر، ایجاد و به‌طور نامناسب مورداستفاده قرار گرفت. اگر نتایج پژوهش‌های ورویی و میرزکی (۱۳۹۰)، اسماعیلی (۱۳۹۰) و رضوی (۱۳۸۶) مبنی بر «بخشی از شیوه‌های مقابله با کلاهبرداری رایانه‌ای نیازمند ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان‌ها در مورد مخاطرات سامانه‌های رایانه‌ای است و نظارت دائمی سازمان‌ها بر سامانه‌های رایانه‌ای بر تدابیر امنیتی از قبیل حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت اطلاعات در مقابله با کلاهبرداری رایانه‌ای، شناخت کافی از علم رایانه، افزایش سرمایه‌گذاری و توسعه فناوری‌های جدید از اهمیت ویژه‌ای برخوردار است»، موردتوجه ذینفعان قرار می‌گرفت، شاهد این‌گونه توزیع و تراکم کلاهبرداری برداشت‌های غیرمجاز از شهروندان در مناطق مختلف شهر تهران نبودیم.

## منابع


- احمدی، سجاد؛ سیف‌الدینی، فرانک؛ کلانتری، محسن (۱۳۹۲). تحلیل فضایی الگوهای بزهکاری در منطقه ۱۷ شهرداری تهران. نشریه تحقیقات کاربردی علوم جغرافیایی. سال (۱۳)، شماره (۳۱)، ص (۷۲-۴۷).
- اس.وال، دیوید (۱۳۹۴) جرائم رایانه‌ای: تغییر ماهیت جرم در عصر اطلاعات (ابوذر اورکی، مترجم). تهران: دانشگاه علوم انتظامی امین.
- اسمعیلی، حبیبه (۱۳۹۰). ظهور سرمایه‌گذاری‌های جدید و چالش‌های پلیس. فصلنامه دانش انتظامی آذربایجان شرقی. سال (۱)، شماره (۲)، ص (۲۶-۳۵).
- اکبری، الهه؛ اصانلو، علی؛ معتمدی راد، محمد؛ پورهاشمی، سیما (۱۳۹۲). نقش علوم زمین قانونی در بررسی جرائم و اجرای قانون. مطالعات بین‌المللی پلیس. سال (۵)، شماره (۱۵)، ص (۸۴۹۶).
- توان‌بخش، جعفر؛ دوستار، محمد؛ قیاسی، رضا (۱۳۹۶). تحلیل راهکارهای مواجهه با فعالیت‌های فیشینگ در بانکداری الکترونیکی. فصلنامه پژوهش‌های اطلاعاتی و جنایی. سال (۱۲)، شماره (۱)، ص (۱۱۱-۱۳۲).
- جی راش، جاناتان (۱۳۷۹). کلاهبرداری اینترنتی. پژوهش‌های ارتباطی. شماره (۲۱-۲۲).
- رضوی، محمد (۱۳۸۶). جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آن‌ها. فصلنامه دانش انتظامی. سال (۹)، شماره (۱)، ص (۱۲۰-۱۴۰).
- روضه‌ای، منصور؛ توان‌بخش، جعفر؛ حسن‌زاده، حمید (۱۳۹۶). ابزارهای پیشگیری از جرائم نوظهور در فضای مجازی. فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی. شماره (۵۰)، ص (۱-۲۲).
- شکوئی، حسین (۱۳۸۲). اندیشه‌های نو در جغرافیا (جلد ۱). تهران: انتشارات گیتاشناسی.
- صادقی، رضا؛ زنجری، نسیبه (۱۳۹۶). الگوی فضایی نابرابری توسعه در مناطق (۲۲) گانه کلان‌شهر تهران. فصلنامه علمی پژوهشی رفاه اجتماعی. سال (۱۷)، شماره (۹۶)، ص (۱۴۹-۱۸۴).
- عبادی‌نژاد، سیدعلی؛ امینی، داود (۱۳۹۴). مبانی جغرافیای انتظامی. سازمان تحقیقات و مطالعات ناجا.
- قربانی سپهر، آرش؛ انصاری، زهرا؛ سلطانی محمد، زهرا (۱۳۹۷). نقش سیستم اطلاعات جغرافیایی در توسعه امنیت پایدارشهری. فصلنامه علمی تخصصی دانش انتظامی خراسان‌رضوی. سال (۴۰)، شماره (۱۰)، ص (۱۷۳-۲۰۴).

کلانتری، محسن؛ توکلی مهدی (۱۳۸۶). شناسایی کانون‌های جرم‌خیز شهری. فصلنامه مطالعات پیشگیری از جرم. سال (۲)، شماره (۲)، ص (۷۶-۱۰۰).

- نتزگر، مایکل؛ موراسی، جرمی (۱۳۹۴). تحقیقات در جرائم با فناوری پیشرفته (مهدی جاوید، مترجم) تهران: دانشگاه علوم انتظامی امین.
- ورویی، اکبر؛ میرزکی، سید شمس‌الدین (۱۳۹۰). بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه‌ای پلیس آگاهی تهران سال ۱۳۸۶-۱۳۸۷. فصلنامه کارآگاه. سال (۴)، شماره (۱۴)، ص (۶۲-۸۷).
- ورویی، اکبر؛ میرزکی، سید شمس‌الدین (۱۳۹۰). بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه‌ای.فصلنامه علمی ترویجی کارگاه. سال (۲)، شماره (۱۴)، ص (۶۲-۸۷).
- وکیلی، شیدا (۱۳۹۵). کلاهبرداری اینترنتی. کنفرانس جهانی روانشناسی و علوم تربیتی، حقوق و علوم اجتماعی در آغاز هزاره سوم.
- هدایتی، حمید (۱۳۹۳). بررسی تجارت الکترونیک و جرم کلاهبرداری اینترنتی (پایان‌نامه کارشناسی‌ارشد). سمنان: دانشگاه آزاد واحد شاهرود.
- هیرشفلید، الکس؛ باورز، کیت (۱۳۹۵). نقشه‌سازی و تحلیل داده‌های جرائم (اکبر ورویی و حمید فاطمی، مترجم). تهران: دانشگاه علوم انتظامی امین.
- Ahmed Aleroud, Lina Zhou (2017). Phishing environments, techniques, and countermeasures: a survey, Computers & Security, pp1-46. http://dx.doi.org/doi:10.1016/j.cose.2017.04.006.
- Azeem Aleem and Albert Antwi-Boasiako (2011). Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat.International Journal of Law, Crime and Justice. 39, pp 140-160.doi:10.1016/j.ijlcj.2011.05.003.
- Bhavna Arora (2016).Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science. (8), pp 540—542. http://dx.doi.org/10.1016/j.pisc.2016.06.014.
- C. RICHARD BAKER (2002).CRIME, FRAUD AND DECEIT ON THE INTERNET: IS THERE HYPERREALITY IN CYBERSPACE? Critical Perspectives on Accounting. 13, pp 1–15. doi:10.1006/cpac.2001.0494.
- Holtjona Galanxhi and Fiona Fui-Hoon Nah (2007).Deception in cyberspace: A comparison of text-only vs. avatar-supported medium. Int. J. Human-Computer Studies 65, pp 770–783. doi:10.1016/j.ijhcs.2007.04.005.C
- INTERNET SCAM ARTISTS. Computer Fraud & Security Bulletin.p8.

Johannes M. Bauer and Michel J.G. van Eeten (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy. 33, pp 706–719. doi:10.1016/j.telpol.2009.09.001.

- Kim-Kwang Raymond Choo (2011).The cyber threat landscape: Challenges and future research directions. computers & s e c u rity. 3 0, pp 7 1 9 -7 3 1. doi:10.1016/j.cose.2011.08.004.
- Maskun, Alma Manuputty, S.M.Noor, Juajir Sumardi (2013). CYBER SECURITY: RULE OF USE INTERNET SAFELY?. 13th International Educational Technology Conference. 103. pp 255 – 261.doi: 10.1016/j.sbspro.2013.10.333.
- Nalin Asanka Gamagedara Arachchilage& Steve Love (2014).Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 38,pp 304–312. http://dx.doi.org/10.1016/j.chb.2014.05.046.
- Peggy E. Chaudhry (2016).The looming shadow of illicit trade on the internet. Business Horizons. (13),pp1-13.http://dx.doi.org/10.1016/j.bushor.2016.09.002.
- Pete Simpson. (2003).Spoofed Identities: Virus, Spam or Scam?. Computer Fraud & Securit. (10):6-8. DOI: 10.1016/S1361-3723(03)10006-1.
- Phillip Hallam-Baker (2005).Prevention strategies for the next wave of cyber crime.Network Security. (10), pp12-15.https://doi.org/10.1016/S1353-4858(05)70291-9.
- Robert J.FischerEdward P.HalibozekDavid C.Walters (2019). Selected Security Threats of the 21st Century. Introduction to Security (Tenth Edition).pp487-505. https://doi.org/10.1016/B978-0-12-805310-2.00019-6
- Rodger Jamieson,Lesley Pek Wee Land, Donald Winchester,Greg Stephens,Alex Steel, Alana Maurushat,dick Sarre(2012).Addressing identity crime in crime management informationsystems: Definitions, classification, and empirics.computer law& security review.2 8,pp3 8 1 -3 9 5. doi:10.1016/j.clsr.2012.03.013.
- Seung Yeop Paek and Mahesh K. Nalla (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. International Journal of Law, Crime and Justice. 43, pp 626e642.http://dx.doi.org/10.1016/j.ijlcj.2015.02.003.
- Seung Yeop Paek and Mahesh K.Nalla(2015).The relationship between receiving phishing attempt and identity theft victimization in South Korea**.** International Journal of Law, Crime and Justice.43(4)pp 626-642. https://doi.org/10.1016/j.ijlcj.2015.02.003
- Shuyuan Mary Ho, Paul Benjamin Lowry, Merrill Warkentin, Yanyun Yang, Jonathan M. Hollister (2016). Gender deception in asynchronous online communication: A path analysis. Information Processing and Management.pp 1–21. http://dx.doi.org/10.1016/j.ipm.2016.06.004.
- Soudabeh Vahdati and Niloofar Yasini (2015).Factors affecting internet frauds in private sector: A case study in Cyberspace Surveillance and Scam Monitoring

Agency of Iran. Computers in Human Behavior.51, 180-187. http://dx.doi.org/10.1016/j.chb.2015.04.058

- Taiwo A. Oriola (2005).Advance fee fraud on the Internet: Nigeria's regulatory response. Computer Law & Security Report. (21), pp 237-248. doi:10.1016/j.clsr.2005.02.006.
- Thomas Kaneshige(1995) CYBERSPACE GENERAL TARGETS
- Tyler Moore (2010).The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection3.3(3-4), pp 1 0 3 – 1 1 7.doi:10.1016/j.ijcip.2010.10.002.