فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی، شماره ۵۰، تابستان ۹۶

ابزارهای پیشگیری از جرایم نو ظهور در فضای مجازی

منصور روضه ای[۱]، جعفر توانبخش[۲]، حمید حسن زاده کرد احمد[۳]

از صفحه ۱ تا ۲۲

تاریخ دریافت : ۹۵/۱۱/۱۳
تاریخ پذیرش:۹۶/۲/۳

چکیده

این تحقیق بررسی ابزارهای پیشگیری از جرایم نو ظهور در فضای مجازی را مورد بررسی قرار میدهد. جامعه آماری این پژوهش تعدادی از قربانیان کلاهبرداری اینترنتی بوده که بر اساس روش نمونه گیری ساده و بر اساس فرمول کوکران مشتمل بر ۱۶۶ نفر انتخاب گردیدند. روش پژوهش از لحاظ هدف کاربردی، از لحاظ چگونگی جمع آوری اطلاعات از جمله پژوهش های توصیفی و از میان انواع پژوهش های توصیفی جز تحقیقات تحلیلی می باشد. ابزار پژوهش شامل پرسشنامه سین وی لی بود که در این پژوهش برای تضمین روایی پرسشنامه از روایی صوری محتوایی و جهت بررسی پایایی ابزار از ضریب آلفای کرونباخ استفاده شده که مقدار ضریب آلفای به دست آمده در گروه خبرگان ۰/۷۸۷ و در گروه قربانیان جرم کلاهبرداری ۰/۸۱۵ می باشد که از نظر آماری مورد قبول است و بنابرین پرسشنامه پایایی لازم را دارد. نتایج به دست آمده از سمت گروه خبرگان نشان می دهد که آیتم های آموزش و آگاه سازی کاربران اینترنت در خصوص کلاهبرداری اینترنتی (مربوط به فرضیه دوم)، آموزش کاربران در خصوص خدمات بانکداری الکترونیک توسط بانک ها (مربوط به فرضیه دوم)، و استفاده از نرم افزارهای امنیتی و ضد جاسوس افزارها توسط کاربران (مربوط به فرضیه چهارم) بیشترین تاثیر را در کاهش کلاهبرداری اینترنتی داشته اند. نتایج به دست آمده از سمت گروه کاربران (قربانیان جرم کلاهبرداری اینترنتی) نشان می دهد که بیشترین تاثیر از بین عوامل شامل: اولویت اول انجام احراز هویت و پروسه های تصدیق هویت داشته(فرضیه سوم)۰ اولویت دوم افزایش سطح آگاهی و آموزش کاربران (فرضیه اول) ؛ اولویت سوم استفاده از ابزارهای امنیتی (فرضیه چهارم) می باشند.

واژه های کلیدی : جرایم سایبری، کلاهبرداری اینترنتی،تجارت الکترونیک، احراز هویت، پیشگیری از جرم، فناوری اطلاعات

---

۱. دانشجوی دکترای حسابداری و عضو هیئت علمی دانشگاه علوم انتظامی امین-نویسنده مسئول. man.phd.acc@gmail.com

۲. کارشناس ارشد مدیریت فناوری دانشگاه آزاد اسلامی تهران مرکز.

۳. کارشناس ارشد مدیریت استراتژیک دانشگاه آزاد اسلامی ساوه.

مقدمه

با گسترش فضای سایبر و ورود اینترنت به زندگی بشر و گره خوردن بسیاری از بخش های زندگی روزمره با آن بسیاری از امورات و خدمات اجتماعی و فضای کسب و کار نیز با آن عجین شده است. در گذشته مراودات تجاری اغلب به صورت سنتی بوده که در این بین بعضا مجرمان با ورود به صحنه کسب و کار و تجارت اقدام به کلاهبرداری به شیوه سنتی می نمودند. ضررهای مالی متوجه افراد می گردید همزمان با ورود فناوری اطلاعات علی الخصوص اینترنت به صحنه کسب و کار و تجارت نحوه مراودات تجاری و خرید و فروش نیز دستخوش تغییرات بسیاری گردید. به طوری که میتوان ادعا نمود هم اکنون بخش اعظم مراودات مالی و تجاری از طریق اینترنت صورت می پذیرد. از سوی دیگر با در دسترس قرار گرفتن ابزارهایی چون وب سایت ها ،پست الکترونیک، بانکداری الکترونیک ، شبکه های اجتماعی و وب تعاملی تغییرات در زمینه مبادلات تجاری ، خرید و فروش کالا و .. به وجود آمده است. به گونه ای که در بسیاری از کشورها فروشگاه های آنلاین از رونق بسیاری برخوردار بوده و بسیاری از افراد خرید و فروش را از این طریق به انجام می رسانند. این عمل باعث کاهش هزینه ، صرفه جویی در وقت می گردد.

در گذشته بسیاری از تجار و افراد به منظور ارسال یک پیش فاکتور ساده مجبور به ارسال آن از طریق پست و یا فکس بودند اما در حال حاضر به مدد اینترنت و پست الکترونیک قادر به انجام مراودات خود در چند ثانیه می باشد. لذا اینترنت و فناوری با کاهش هزینه ها وافزایش سرعت در انجام فعالیت های تجاری محدودیت ها ی زمانی و مکانی را رفع نموده است . با تبدیل شیوه های سنتی به شیوه های نوین در انجام فعالیتهای تجاری و اقتصادی ،جرایم و مجرمین نیز تغییر نموده به گونه ای که مجرمین نیز با بهره گیری از ویژگی ها و تسهیلاتی که فناوری در اختیار قرار داده سعی در رسیدن به اهداف و ومطامع خود نموده و از فناوری به جهت رسیدن به اهداف خود و انجام جرایم استفاده می کنند. به گونه ای که مجرمین نیز با مجرمین سنتی متفاوت بوده و مجرمین حوزه فناوری اطلاعات افرادی با هوش و صاحب دانش می باشند. و این افراد در حال حاضر با شیوه های نوین و با استفاده از اینترنت اقدام به کلاهبرداری

می نمایند که باعث به وجود آمدن واژه جدیدی به نام کلاهبرداری اینترنتی گردیده که با کلاهبرداری سنتی متفاوت بوده و اینترنت ابزار اصلی برای انجام این جرم می باشد. کلاهبرداری های اینترنتی باعث ضررهای اقتصادی بسیاری به تجار، صرافان و افراد گردیده است و تبدیل به یک معضل بزرگ در تجارت الکترونیک و مراودات تجاری روزمره افراد گردیده به گونه ای که بسیاری از کشورهای جهان را درگیر نموده و باعث گردیده که آنان فعالانه به دنبال راهکارهایی برای پیشگیری و مقابله با این پدیده باشند.

درادامه مقاله پس از بررسی اجمالی موضوع ابزارهای پیشگیری از جرایم نو ظهور در فضای مجازی و اجزای تشکیل دهنده آن، به بررسی شاخص های مرتبط با متغیرهای مورد مطالعه پرداخته می شود. به دنبال تشریح روش شناسی پژوهش، یافته های اصلی پژوهش توضیح داده می شود و در نهایت پس از بحث و بررسی و نتیجه گیری، مقاله با ارائه چند پیشنهاد عملی به پایان می رسد.

بیان مساله

تمایل روز افزون کاربران به استفاده از فناوری های پیشرفته از جمله رایانه و اینترنت وورود به عرصه تجارت الکترونیک زمینه مساعدی برای ظهور و بروز جرایم سایبری یا اینترنتی به وجود آورده است. با توجه به بدون مرز بودن جرایم فضای سایبر و اینترنت و عدم وجود مرز فیزیکی مجرمان در هر نقطه ای از جهان میتوانند در نقطه ای دیگر که لزوما در محل زندگی فرد مجرم نمی باشد مرتکب جرم گردند و از سویی نیز مجرمان این حوزه صاحب دانش بوده و هر روزه از تکنیک ها و روش های جدید و نوظهور مبتنی بر فناوری اطلاعات برای ارتکاب جرم استفاده میکنند و به همین دلیل مراجع قضایی و انتظامی برای پیشگیری از این جرایم و کشف آن ها با چالش های نوینی مواجه هستند. مجرمان به منظور کلاهبرداری اینترنتی از شیوه های گوناگونی استفاده می کنند که یکی از رایج ترین روشها در بین مجرمین کلاهبرداری از طریق سرقت هویت است که در این شیوه مجرمین به منظور سرقت اطلاعات مالی و هویتی افراد از شگردهای مختلفی استفاده می کنند که از آن جمله می توان به موارد زیر اشاره نمود.

سرقت هویت از طریق نفوذ به پایگاه های داده

- سرقت هویت از طریق فیشینگ
- سرقت هویت از طریق مهندسی اجتماعی
- سرقت هویت از طریق جاسوس افزارها و کیلاگرها

از دیگر شیوه‌های کلاهبرداری اینترنتی که توسط مجرمان مورد استفاده قرار می گیرند میتوان به کلاهبرداری از طریق جعل ایمیل‌های تجاری،کلاهبرداری از طریق وب سایت‌های مزایده آنلاین، کلاهبرداری ۴۱۹ نیجریه ای، کلاهبرداری از طریق دوستی و عشق اینترنتی، کلاهبرداری از طریق فروش کالای تقلبی و یا عدم تحویل کالا اشاره نمود که بسیاری از جنبه‌های فنی و اجتماعی این شیوه‌های کلاهبرداری اینترنتی برای کاربران نامشخص است بنابراین بسیاری از آنان گرفتار و قربانی این نوع جرم می گردند و از سویی نیز برخی دستگاههای متولی در این حوزه نیز درک روشنی از موارد یاد شده جهت انجام وظایف ذاتی خود ندارند . بنابراین بررسی این معضل و ارائه راهکارهایی جهت مقابله با این پدیده میتواند راهگشا باشد در گذشته مطالعاتی جزئی در این حوزه صورت پذیرفته و راهکارهایی ناقص در خصوص راهکارهای مقابله با کلاهبرداری اینترنتی ارائه گردیده‌اند .لذا مسئله پژوهش بررسی جرم کلاهبرداری اینترنتی و شناسایی و ارائه راهکارها و ابزارهای پیشگیری از این جرم می‌باشد. لذا سوالات پژوهش را می توان به شرح زی بیان نمود:

۱. راهکارها و ابزارهای پیشگیری از کلاهبرداری اینترنتی چیست؟
۲. استفاده از نرم افزارهای امنیتی چه تاثیری بر پیشگیری از کلاهبرداری اینترنتی دارد؟
۳. آگاه سازی و آموزش کاربران چه تاثیری بر پیشگیری از کلاهبرداری اینترنتی دارد؟
۴. استفاده از راهکارهای فنی چه تاثیری بر پیشگیری از کلاهبرداری اینترنتی دارد؟
۵. یشرفت خدمات فناوری اطلاعات چه رابطه ای با افزایش کلاهبرداری اینترنتی دارد؟

مبانی نظری تحقیق

ادبیات موضوع

در رابطه با روش‌ها و راهکارهای پیشگیری از کلاهبرداری اینترنتی از سوی محققان شیوه‌ها و راهکارهای مختلفی در حوزه پیشگیری وضعی و اجتماعی از

جرم پیشنهاد شده است. از سوی دیگر با توجه به این مسئله که جرایم سایبری اغلب بر پایه فناوری اطلاعات به وقوع می پیوندند و روالهای مجرمانه آنها در فضای مجازی سپری می گردد، لذا رویکردهای پیشگیرانه مبتنی بر فناوری اطلاعات می تواند تاثیر زیاد و موثرتری در پیشگیری از وقوع و ارتکاب جرایم سایبری داشته باشد. در این بخش به برخی از روشها و راهکارهای مهم از دیدگاه محققان در پیشگیری از جرم کلاهبرداری اینترنتی پرداخته می شود.

فضای سایبر

فضای سایبر ، فضای مجازی است که ارتباطات انسانها از طریق فن آوری اطلاعات و بدون محدودیت های جغرافیایی برقرار می شود. مثلا در یک سیستم آنلاین گفتگو که افراد از طریق شبکه رایانه ای با یکدیگر ارتباط برقرار کنند، نمونه ای از فضای سایبر است. برخی محققان فضای سایبر را با حالتهایی از ناهوشیاری و رؤیا قابل قیاس می دانند و شباهتهایی را در این بین بیان نموده اند. در فضای سایبر یک کاربر بدور از واقعیت ها و قوانین دنیای فیزیکی قدم درون دنیایی می گذارد که واقعیت های متفاوت که غالبا پروژه ذهن اشخاص است پیش روی دارد. شما در فضای مجازی حالتهای متنوع و متفاوت ذهنی را از قبیل تخیلات، خیال پردازی ها، توهمات، حالات هیپنوتیستیک و سطوح گوناگونی از هوشیاری را تجربه می کنید. تحت این شرایط فضای سایبر همانند دنیای «رویا» می شود. دنیایی که وقتی ما بخواب می رویم پدیدار می شود(سید مفیدی ۱۳۸۳).

جرم[1]

انجام هر نوع رفتار یا ترک رفتاریست که قانون را نقض می کند و مجازات در پی دارد. اهمیت نسبی جرایم مختلف و شیوه کیفر دادن فعالیت های مجرمانه؛ در طول تاریخ و در جوامع مختلف، متفاوت بوده است.

کلاهبرداری اینترنتی[2]

کلاهبردای اینترنتی به هر نوع طرح متقلبانه ای گفته می شود که یک یا چند بخش از اینترنت را به کار می گیرد و تا در خواست های متقلبانه ای را به منظور

۱. Crime

۲. Internet Fraud

بـردن امـوال و احتمـالا « انجـام معامـلات جعلـی بـا قربانیـان احتمالـی مطـرح سـازد. بنابرایـن مشـخص می‌شـود کـه کلاهبـرداری اینترنتـی از زمانـی رواج پیـدا کـرد کـه محیـط مجـازی مثـل محیـط اینترنـت پـا بـه عرصـه وجـود گذاشـت و تقریبـا» حـدود دو دهـه اسـت کـه از عمـر ایـن جـرم می گـذرد)عباسـعلی، ۱۳۹۰).

تصدیق هویت[1]

تعییـن صحـت و سـقم یـک ویژگـی، داده یـا نهـاد گفتـه می‌شـود. ایـن فراینـد ممکـن اسـت شـامل تاییـد هویـت یـک شـخص، دنبـال کـردن ریشـه‌های یـک سـازه بشـری، مطمئـن شـدن از اینکـه یـک کالا همانـی اسـت کـه بسـته‌بندی ادعـا می کنـد، یـا اطمینـان از قابـل اعتمـاد بـودن یـک نرم‌افـزار رایانـه‌ای باشد)عباسـعلی، ۱۳۹۰)..

عناصر اجتماعی تاثیر گذار در جرم کلاهبرداری اینترنتی

عـدم اطـلاع رسـانی و آگاهـی بخشـی بـه کاربـران اینترنـت و عـدم دقـت آنهـا بـه علـت عـدم دریافـت آموزشـهای پیشـگیرانه از سـوی دسـتگاهها و سـازمانهای مربوطـه منجـر بـه افزایـش وقـوع جـرم کلاهبـرداری اینترنتـی می‌شـود کـه بـا آمـوزش و اطـلاع رسـانی مناسـب بـه کاربـران میتـوان بـه سـوی کاهـش ایـن جـرم قـدم برداشـت.

عناصر فنی تاثیر گذار در افزایش جرم کلاهبرداری اینترنتی

عــدم اســتفاده از نــرم افزارهــا و ســخت افزارهــای امنیتــی بــه روز شــده و نیــز پروســه‌های تصدیــق هویــت منجــر بــه افزایــش وقــوع جــرم کلاهبــرداری اینترنتــی می‌شـود کـه بـا بـه کارگیـری مـوارد یـاد شـده توسـط کاربـران می تـوان از وقـوع کلاهبــرداری اینترنتــی پیشــگیری نمــود.

پیشینه تحقیق‌های انجام شده

پیشینه داخلی

- مسـعود بوربـور در سـال ۱۳۹۳ در پایـان نامـه کارشناسـی ارشـد خـود بـا عنـوان» تبییـن شـیوه‌های مبتنـی بـر فنـاوری اطلاعـات بـرای پیشـگیری از کلاهبرداری‌هـای مالـی موجـود در فضـای مجـازی» بـه بیـان شـیوه‌هایی جهـت مقابلـه و پیشـگیری از کلاهبرداری‌هـای مالـی موجـود در فضـای مجـازی پرداختـه اسـت. نتایـج محقـق نشـان داد کـه شـیوه‌های مبتنـی بـر فنـاوری اطلاعـات بـرای پیشـگیری از

۱. Authentication

کلاهبرداری‌های مالی موجود در فضای مجازی موثر است.

- عباسعلی اکبری در سال ۱۳۹۰ در مقاله ای با عنوان «کلاهبرداری رایانه ای جلوه ای نوین و متمایز از کلاهبرداری سنتی» در همایش منطقه ای چالش‌های جرایم رایانه ای در عصر امروز به بررسی جرم کلاهبرداری رایانه ای و مقایسه آن با کلابرداری سنتی پرداخته است. . نتایج محقق نشان داد که کلاهبرداری رایانه ای متمایز از کلاهبرداری سنتی می‌باشد.
- ساعدی در سال ۹۲ در پایان نامه کارشناسی ارشد خود با عنوان «بررسی راهکارهای پیشگیری اجتماعی از کلاهبرداری سایبری» در دانشگاه آزاد واحد تهران شمال ، برخی از راهکارهای اجتماعی را در خصوص پیشگیری از کلاهبرداری سایبری بررسی نموده است.
- حسین میر محمد صادقی و محمد رسول شایگان در سال ۱۳۸۶ و در مقاله ای تحت «عنوان راهکارهای مقابله با جرم کلاهبرداری رایانه ای در حقوق کیفری ایران» منتشر شده در مجله دیدگاههای حقوق قضایی به موضوع ایجاد فرهنگ بهره گیری از رایانه و آگاه ساختن افراد و سازمان‌ها در مورد مخاطرات سیستم‌های رایانه‌ای پرداخته‌اند و همچنین نظارت دائمی سازمان‌ها بر روی سیستم‌های رایانه‌ای و تدابیر امنیتی از قبیل حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت اطلاعات در مقابله با کلاهبردای رایانه‌ای را مهم برشمرده‌اند.
- حبیب سالارزهی، محمدجواد جمشیدی ،محمد جعفر جمشیدی در سال ۱۳۹۰ در مقاله ای با عنوان «مدل یشنهادی مقابله با جرایم رایانه ای در همایش منطقه ای چالش‌های رایانه ای در عصر امروز» به ارائه مدل در خصوص مقابله و پیشگیری از جرایم رایانه ای از جمله کلاهبرداری رایانه ای پرداخته‌اند .در این مدل و با مد نظر قرار دادن دو نوع استراتژی که قابلیت پیاده سازی بصورت همزمان را نیز دارا می‌باشند ، در مرحله ی اول سعی می‌شود تا از وقوع جرایم رایانه ای جلوگیری شود بدین صورت که از استراتژی دفاعی بهره گرفته می‌شود . در استراتژی دفاعی باید نرم افزارهای امنیتی (ضد ویروس ، ضد جاسوسی و ...) بر روی سیستم‌های کامپیوتری سازمان نصب شده و از فناوری‌های ایمن سازی شبکه مثل استفاده از دیواره آتش و نیز گواهی‌های

امنیتی همچون SSL برای وب سایت سازمان ، بهره جست. همچنین برای مقابله با جرایم رایانه ای غیر فنی اقدام به آموزش کارکنان و مشتریان سازمان کرد.

پیشینه خارجی

- کیت فارینا[1] در سال ۲۰۱۵ و در مقاله ای با عنوان «سرقت هویت» به بررسی این شیوه از کلاهبرداری اینترنتی پرداخته و برخی نکات امنیتی را به منظور جلوگیری از سرقت هویت ذکر نموده است.
- آجیت سینگ[2]، آوادش بهارواج[3] و دنگایاچ[4] (۲۰۱۵) در مقاله ای تحت عنوان «پیشگیری از جرایم سایبری» در اولین کنفرانس بین المللی تحقیقات میان رشته ای ضمن تشریح برخی از جرایم سایبری ازجمله کلاهبرداری اینترنتی برخی راهکارها از جمله استفاده از فایروال، فیلتر نمودن ایمیل ها،عدم پاسخگویی به ایمیل های ناشناس، عدم بازنمودن فایلهای پیوستی مشکوک، پشتیبان گیری اطلاعات، ویروس کشی مرتب سیستم ها، را برای پیشگیری از جرایم سایبری ذکر کرده اند.
- لاکشانا پراسانتی[5] در سال ۲۰۱۵ در مقاله خود با عنوان « تشخیص و پیشگیری از جرایم سایبر» در ژورنال بین المللی تحقیات پیشرفته در کامپیوتر و مهندسی ارتباطات به بررسی انواع جرایم سایبری پرداخته و راهکارهایی چون استفاده از تکنولوژی رمز نگاری ، استفاده از پروتکل های رمز شده، استفاده از دستگاههای رمز یاب سخت افزاری، استفاده از نرم افزارها و سخت افزارهای امنیتی را به منظور پیشگیری از جرایم سایبری ارائه نموده است.
- سیدنی تسانگ[6] «در مقاله ای با عنوان شناسایی کلاهبرداری های جمعی در مزایده آنلاین» که در کنفرانس بین المللی کامپیوتر و ارتباطات و در سال ۲۰۱۵ ارائه گردیده به بررسی پدیده کلاهبرداری اینترنتی از طریق مزایده آنلاین پرداخته و روش هایی را برای کشف آنها ذکر نموده است.

---

۱. Katie A. Farina

۲. Ajeet Singh

۳. Awadesh Bhardwaj

۴. Dangayach

۵. Lakshmi Prasanthi

۶. Sidney Tsang

- مونیکا ویتی[1] و تام بوچانان[2] در مقاله مشترک خود در سال ۲۰۱۵ با عنوان « کلاهبرداری اینترنتی از طریق عشق اینترنتی: یک جرم سایبری مهم» در ژورنال روان شناسی سایبر و شبکه های اجتماعی به بررسی کلاهبرداری روبه رشد از طریق عشق اینترنتی و نقش سایت های دوست یابی در آن پرداخته و راهکارهایی برای مقابله با آن ارائه نموده اند.
- سین وی لی[3]، حمید جهانخانی و عمران عسکرنیا نیز در مقاله ای در سال ۲۰۱۲ با عنوان «آموزش، آگاهی بخشی و اطلاع رسانی در مدل ۴ بعدی پیشگیری از جرایم سایبری» یک مدل را در خصوص پیشگیری از جرایم سایبری ارائه نموده اند که آموزش کاربران و آگاهی بخشی به آنان از ارکان این مدل می باشد و تاثیرات آنها در پیشگیری از جرایم سایبری بررسی نموده اند. این مدل برگرفته از نظریه پیشگیری وضعی است که قابلیت انجام در سطوح مختلف از جمله اشخاص ، اجتماع، و محیط فیزیکی را دارد.

اهداف تحقیق

الف) اهداف اصلی

شناسایی راهکارها و ابزارهای پیشگیری از کلاهبرداری اینترنتی

ب) اهداف فرعی

۱. تبیین شیوه ها و تکنیک های کلاهبرداری اینترنتی
۲. جلوگیری و یا کاهش وقوع جرایم کلاهبرداری اینترنتی با به کارگیری نتایج حاصل از این تحقیق
۳. آموزش کاربران با در نظر گرفتن نتایج حاصل از این تحقیق

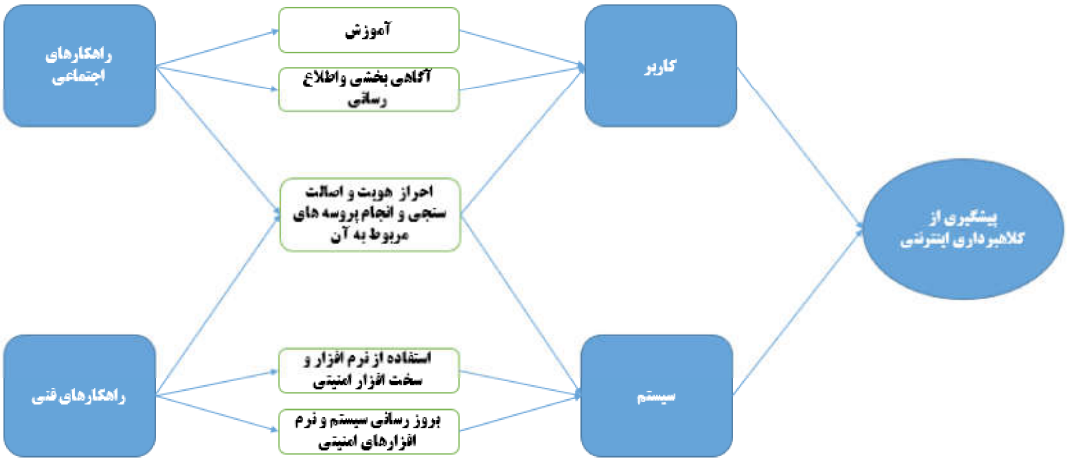
مدل مفهومی تحقیق

با توجه به مطالعات انجام شده، مصاحبه با متخصصان و اساتید دانشگاه، مدل مفهومی سین وی لی (۲۰۱۲) جهت شناسایی ابزارهای پیشگیری از جرایم نو ظهور در فضای مجازی معرفی گردید. آموزش و آگاهی بخشی به کاربران، استفاده از

---

۱. Monica T. Whitty
۲. Tom Buchanan
۳. Sin Wee Lee

ابزارهـای امنیتـی نـرم افـزاری و سـخت افـزاری و بـروز رسـانی آنهـا، احـراز هویـت و اصالـت سـنجی تاثیـر مسـتقیم در پیشـگیری از کلاهبـرداری اینترنتـی دارنـد. برخـی از ایـن عوامـل مربـوط بـه کاربـران اسـت و برخـی بایـد از طریـق سیسـتم صـورت پذیـرد و برخـی از عوامـل و فاکتورهـای تاثیرگـذار همچـون احـراز هویـت در هـر دو مشـترک اسـت لـذا کلیـه عوامـل ذکـر شـده موجـب پیشـگیری از کلاهبـرداری اینترنتـی می گـردد.



فرضیه های تحقیق

- تاثیـر تغییـرات تکنولوژیـک در سـطح خدمـات IT مـورد اسـتفاده کاربـران در کلاهبـرداری اینترنتـی.
- تاثیرافزایش آگاهی و آموزش کاربران بر پیشگیری از کلاهبرداری اینترنتی.
- تاثیراحـراز هویـت (اصالـت سـنجی) و اسـتفاده از پروسـه های تصدیـق هویـت بـر پیشـگیری از کلاهبـرداری اینترنتی .
- تاثیـر اسـتفاده از ابزارهـای امنیتـی(سـخت افـزاری و نـرم افـزاری) در پیشـگیری از کلاهبـرداری اینترنتـی .

روش تحقیق

ایـن تحقیـق ازنظرجهـت گیـری، کاربـردی وازنظـر نـوع پژوهـش، میدانـی وازنظـر راهبـرد پژوهـش، پیمایشـی و از نظـر هـدف پژوهشـی، توصیفـی بـه شـمار مـی رود جامعـه آمـاری ایـن پژوهـش کارشناسـان مبـارزه بـا جرایـم سـایبری، مدیـران ارشـد و کارشناسـان عالـی و ارشـد حـوزه فنـاوری و امنیـت اطلاعـات و کاربرانـی کـه مـورد

کلاهبرداری اینترنتی قرار گرفته‌اند می‌باشد ابزار گرد آوری اطلاعات پرسشنامه لی است که بصورت میدانی انجام شده است و در تحقیق جهت تعیین میزان اعتبارپرسشنامه ازآزمون آلفای کرونباخ و جهت تعیین نرمال بودن داده‌ها ازآزمون کولمونوگروف اسمیرونوف استفاده شده است. در انتها جهت بررسی نحوه انتخاب داده‌ها از آزمون Runs-test استفاده می‌شود .برای تجزیه و تحلیل داده‌ها از آزمون Kmo و پس از بررسی، میزان بار عاملی تعیین می‌شود.

حجم نمونه و نمونه گیری

جامعه آماری این تحقیق از نظر مکانی به دو دسته تقسیم می‌گردد. دسته اول کاربرانی هستند که در سال ۱۳۹۴ در استان تهران قربانی کلاهبرداری اینترنتی گردیده‌اند که تعداد افراد شکایت کننده در حدود ۱۸۰۰ نفر می‌باشد که به دلیل تعدد پرونده‌های ثبت شده و عدم امکان دسترسی به تمام این افراد در راستای ارزیابی صحیح موضوع جامعه آماری را محدود به افرادی ساختیم که در حوزه شهر تهران اقدام به شکایت نموده‌اند که تعدادشان حدود ۲۴۵ نفر می‌باشد که براستفاده از فرمول کوکران تعداد نمونه ۱۵۰ نفر است. دسته دوم خبرگانی هستند که با مسائل مربوط به جرایم سایبری و کلاهبرداری اینترنتی در ارتباط می‌باشند که تعداد آنها ۵۰ نفر می‌باشد .

$$n=\frac{N Z_{\frac{a}{2}}^{2} p(1-p)}{\varepsilon^{2}(N-1)+Z_{\frac{a}{2}}^{2} p(1-p)}$$

ابزارهای جمع آوری اطلاعات

با استفاده از این ابزارها پرسشنامه و روش کتابخانه ای مانند مقالات و کتابها و پایان نامه‌ها و رساله‌های دانشجویان و اساتید دانشگاهی به گردآوری داده‌ها برای تحلیل مدل مفهومی تحقیق استفاده گردیده است. برای گردآوری داده‌های مربوطه از پرسشنامه در دو سطح کاربران (قربانیان کلاهبرداری) و خبرگان مبارزه با جرایم سایبری استفاده شده است . پرسشنامه قربانیان و خبرگان هر یک شامل ۱۸ سوال مرتبط با ۴ فرضیه تحقیق بودند که بر اساس جدول زیر تقسیم بندی شده‌اند.

فرضیه ها	سوالات	جهت گیری سوالات
فرضیه۱: تاثیر تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در کلاهبرداری اینترنتی	۱-۴	میزان ارتباط با وقوع کلاهبرداری
فرضیه ۲: تاثیرافزایش آگاهی و آموزش کاربران بر پیشگیری از کلاهبرداری اینترنتی .	۵-۷	میزان تاثیر بر پیشگیری از کلاهبرداری اینترنتی
فرضیه ۳: تاثیراحراز هویت (اصالت سنجی) و استفاده از پروسه های تصدیق هویت بر پیشگیری از کلاهبرداری اینترنتی .	۸-۱۵	میزان تاثیر بر پیشگیری از کلاهبرداری اینترنتی
فرضیه ۴: تاثیر استفاده از ابزارهای امنیتی(سخت افزاری و نرم افزاری) در پیشگیری از کلاهبرداری اینترنتی .	۱۶-۱۸	میزان تاثیر بر پیشگیری از کلاهبرداری اینترنتی

روایی و پایایی ابزارهای جمع آوری اطلاعات

جهت بالا بردن اعتبار و روایی تحقیق اولا سعی شده تا سئوالات مرتبط با موضوع طراحی شوند و حتی الامکان روان و قابل درک برای پاسخگویان باشد و همچنین پاره ای از توضیحات و تعاریف عملیاتی در ابتدای پرسشنامه به پیشنهاد استاد راهنما صورت گرفته است. ثانیا سعی شده است تا از پرسشنامه های استاندارد قبلی که توسط محققان قبلی مورد استفاده قرار گرفته است، استفاده شود. این پرسشنامه به طور مقدماتی بین ۳۵ نفر توزیع شد تا موارد مجهول و مبهم آن مرتفع و اعتبار و روایی آن بررسی شود. بنابر این روایی پرسشنامه های تحقیق از نوع روایی محتوایی است که پرسشنامه ها بر اساس مبانی نظری تنظیم شده است.همچنین به منظور اطمینان از نتایج حاصله، اقدام به تعیین میزان قابلیت اعتماد (پایایی) پرسشنامه گردید. جهت بررسی میزان پایایی پرسشنامه از نرم افزار SPSS برای بدست آوردن ضریب آلفای کرونباخ استفاده شده است. آلفای کرونباخ یکی از روش های محاسبه قابلیت اعتماد ابزارهای اندازه گیری از جمله پرسشنامه می باشد. هرچه مقدار آلفای کرونباخ به مقدار یک نزدیک تر باشد حاکی از پایایی بالای پرسشنامه است. مقدار ضریب آلفای به دست آمده در گروه خبرگان ۰/۷۸۷ و در گروه قربانیان جرم کلاهبرداری ۰/۸۱۵ می باشد که از نظر آماری مورد قبول است و بنابرین پرسشنامه پایایی لازم را دارد.

آزمون و تحلیل فرضیه‌ها

با توجه به نتایج به دست آمده از آزمون کولمونوگروف اسمیرونوف مشاهده می‌شود که داده‌ها در هر دور گروه خبرگان و کاربران (قربانیان جرم کلاهبرداری) ناپارامتریک بوده و باید از آزمون ناپارامتریک برای سنجش معنی داری داده‌ها استفاده نمود که برای این منظور از آزمون Kmo استفاده خواهد شد . این آزمون پیش شرط انجام آزمون تحلیل عاملی یا تعیین ضرایب عامل‌ها می‌باشد بدین معنی که اگر آزمون انجام شده با مقدار آماره نزدیک به عدد ۱ و سطح معناداری مساوی یا کمتر از ۰/۰۵ باشد می‌توان برای تحلیل دقیق تر فاکتورها به آزمون تحلیل عاملی اکتفا کرد.نتایج به دست آمده از این آزمون برای گروه خبرگان و کاربران (قربانیان جرم کلاهبرداری) به شرح زیر می‌باشد:

گروه خبرگان

جدول آزمون Kmo و نتایج به دست آمده برای گروه خبرگان به شرح زیر می‌باشد:

جدول آزمون معنی داری (kmo) برای گروه خبرگان

آماره Kmo	درجه آزادی(df)	سطح معنی داری(sig)
۰/۸۱۲	۱۵۳	۰/۰۰۰

در جدول فوق مقدار آماره آزمون Kmo در گروه خبرگان برابر با ۰/۸۱۲ بوده و از ۰/۸ بیشتر می‌باشد هم چنین با توجه به اینکه سطح معنی داری در این گروه ۰/۰۰۰ بوده و کمتر از ۰/۰۵ می‌باشد (sig<۰/۰۵) لذا با اطمینان ۹۵ درصد می توان گفت در گروه خبرگان فرضیه H۱ پذیرفته شده و فرضیه H۰ رد می‌شود بنابرین بین عوامل مورد نظر و کلاهبرداری اینترنتی ارتباط معنی دار وجود دارد. و به عبارت دیگر با اطمینان ۹۵ درصد می توان گفت کلیه عوامل ذکر شده در پرسش نامه در کلاهبرداری اینترنتی موثر می‌باشد.

گروه کاربران (قربانیان جرم کلاهبرداری)

جدول آزمون Kmo و نتایج به دست آمده برای گروه کاربران (قربانیان جرم کلاهبرداری) به شرح زیر می‌باشد:

جدول آزمون معنی داری (kmo) برای گروه کاربران (قربانیان جرم کلاهبرداری)

آماره Kmo	درجه آزادی(df)	سطح معنی داری(sig)
۰/۸۰۱	۱۵۳	۰۰۰/۰

در جدول فوق مقدار آماره آزمون Kmo در گروه کاربران (قربانیان جرم کلاهبرداری) برابر با ۰/۸۰۱ بوده و از ۰/۸ بیشتر می‌باشد هم چنین با توجه به اینکه سطح معنی داری در این گروه ۰/۰۰۰ بوده و کمتر از ۰/۰۵ می‌باشد (sig<۰/۰۵) لذا با اطمینان ۹۵ درصد می توان گفت در گروه کاربران (قربانیان جرم کلاهبرداری) فرضیه H۱ پذیرفته شده و فرضیه H۰ رد می‌شود بنابرین بین عوامل مورد نظر و کلاهبرداری اینترنتی ارتباط معنی دار وجود دارد. و به عبارت دیگر با اطمینان ۹۵ درصد می توان گفت کلیه عوامل ذکر شده در پرسش نامه در کلاهبرداری اینترنتی موثر می‌باشد.

تحلیل بار عاملی

بعد از بررسی آزمون kmo باید میزان بار عاملی هر یک از گویه‌ها مشخص شود بدین معنا که با بررسی جدول مربوطه میزان اهمیت هریک از عامل‌ها در شکل گیری متغیر مشخص شود. و برای این منظور از روش تحلیل عاملی استفاده خواهد شد.

گروه خبرگان

برای بررسی بارهای عاملی به جدول ضریب بار عاملی مراجعه می‌نماییم که ضرایب محاسبه شده برای گروه خبرگان به شرح جدول زیر می‌باشد:

جدول ضریب بار عاملی گروه خبرگان

ردیف	شماره فرضیه	عوامل موثر بر کاهش جرم کلاهبرداری اینترنتی	ضریب بار ویژه
۱	فرضیه دوم	نقش افزایش سطح آگاهی و آموزش کاربران (قربانیان جرم کلاهبرداری) در پیشگیری از کلاهبرداری اینترنتی	۸۹۷/۰
۲	فرضیه چهارم	نقش استفاده از ا بزارهای امنیتی (سخت افزار و نرم افزار) در پیشگیری از کلاهبرداری اینترنتی	۷۹۲/۰
۳	فرضیه سوم	نقش انجام احراز هویت و پروسه های تصدیق هویت در پیشگیری از کلاهبرداری اینترنتی	۵۲۰/۰
۴	فرضیه اول	نقش تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در کلاهبرداری اینترنتی	۴۰۸/۰

با استفاده از اطلاعات جدول فوق که در آن فرضیات مطرح شده در تحقیق برای گروه خبرگان ؛ با مقایسه ضریب بارعاملی اولویت بندی شده و فرضیات به ترتیب اولویت آنان در کلاهبرداری اینترنتی ذکر شده‌اند با توجه به اینکه ضرایب محاسبه شده برای عوامل دارای تفاوت معناداری می‌باشند با تعمیم نتایج به دست آمده به جامعه آماری می توان گفت بیشترین تاثیر را از بین عوامل از نظر گروه خبرگان ؛ آموزش و افزایش سطح آگاهی کاربران داشته و استفاده از ابزارهای امنیتی در اولویت دوم ؛ انجام احراز هویت و پروسه‌های تصدیق هویت در رتبه سوم و از نظر گروه خبرگان به ترتیب اهمیت فرضیات دوم و چهارم و سوم در کاهش کلاهبرداری اینترنتی مهم تر از نقش تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در افزایش کلاهبرداری اینترنتی، می‌باشد.

گروه کاربران (قربانیان جرم کلاهبرداری)

برای بررسی بارهای عاملی به جدول ضریب بار عاملی مراجعه می‌نماییم که ضرایب محاسبه شده برای دو گروه کاربران (قربانیان جرم کلاهبرداری) به شرح جدول زیر می‌باشد:

جدول ضریب بار عاملی گروه کاربران (قربانیان جرم کلاهبرداری)

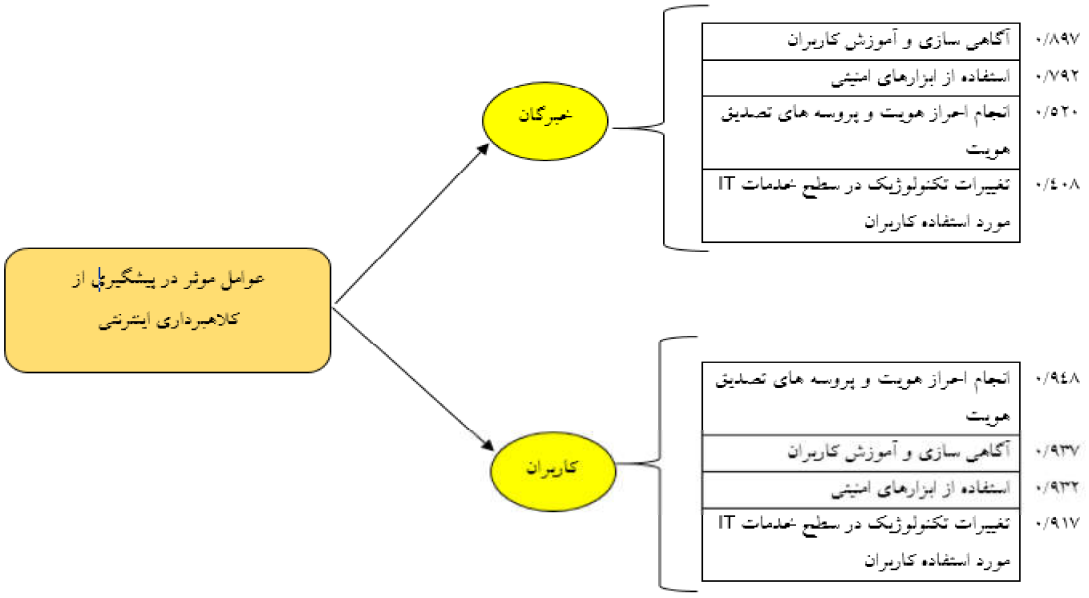
ردیف	شماره فرضیه	عوامل موثر بر کاهش جرم کلاهبرداری اینترنتی	ضریب بار عاملی
۱	فرضیه سوم	نقش انجام احراز هویت و پروسه‌های تصدیق هویت در پیشگیری از کلاهبرداری اینترنتی	۰/۹۴۸
۲	فرضیه دوم	نقش افزایش سطح آگاهی و آموزش کاربران (قربانیان جرم کلاهبرداری) در پیشگیری از کلاهبرداری اینترنتی	۰/۹۳۷
۳	فرضیه چهارم	نقش استفاده از ابزارهای امنیتی (سخت افزار و نرم افزار) در پیشگیری از کلاهبرداری اینترنتی	۰/۹۳۲
۴	فرضیه اول	نقش تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در کلاهبرداری اینترنتی	۰/۹۱۷

با استفاده از اطلاعات جدول فوق که در آن فرضیات مطرح شده در تحقیق برای گروه کاربران (قربانیان جرم کلاهبرداری)؛ ضرایب محاسبه شده برای عوامل تفاوت چندانی نداشته و نمی توان به صورت قطعی اولویت خاصی را مشخص نمود اما با اغماض می توان گفت بیشترین تاثیر را از بین عوامل از

نظر گروه کاربران (قربانیان جرم کلاهبرداری)؛ انجام احراز هویت و پروسه های تصدیق هویت داشته و افزایش سطح آگاهی و آموزش کاربران در اولویت دوم ؛ استفاده از ابزارهای امنیتی رتبه سوم و از نظر گروه کاربران به ترتیب اهمیت فرضیات دوم و چهارم و سوم در کاهش کلاهبرداری اینترنتی مهم تر از اهمیت تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در افزایش کلاهبرداری اینترنتی، می باشد.

مدل تحلیلی

مدل تحلیلی تحقیق با استفاده از ضرایب بار عاملی و نرم افزار EQS برای دو گروه خبرگان و کاربران (قربانیان جرم کلاهبرداری) به شرح زیر می باشد:



نتیجه گیری

نتایج به دست آمده از سمت گروه خبرگان

مقدار آماره آزمون Kmo در گروه خبرگان برابر با ۰/۸۱۲ بوده و از ۰/۸ بیشتر می باشد هم چنین با توجه به اینکه سطح معنی داری در این گروه ۰/۰۰۰ بوده و کمتر از ۰/۰۵ می باشد (sig<۰/۰۵) لذا با اطمینان ۹۵ درصد می توان گفت در گروه خبرگان فرضیه H۱ پذیرفته شده و فرضیه H۰ رد می شود بنابرین بین عوامل مورد نظر و کلاهبرداری اینترنتی ارتباط معنی دار وجود دارد. و به عبارت دیگر با اطمینان ۹۵ درصد می توان گفت کلیه عوامل ذکر شده در پرسش

نامه در کلاهبرداری اینترنتی موثر می‌باشد. با مقایسه ضریب بارعاملی، فرضیات اولویت بندی شده و فرضیات به ترتیب اولویت آنان در کلاهبرداری اینترنتی ذکر شده‌اند با توجه به اینکه ضرایب محاسبه شده برای عوامل دارای تفاوت معناداری می‌باشند با تعمیم نتایج به دست آمده به جامعه آماری می توان گفت بیشترین تاثیر را از بین عوامل از نظر گروه خبرگان ؛ آموزش و افزایش سطح آگاهی کاربران (فرضیه دوم) داشته و استفاده از ابزارهای امنیتی (فرضیه چهارم) در اولویت دوم ؛ انجام احراز هویت و پروسه‌های تصدیق هویت در رتبه سوم (فرضیه سوم) و از نظر گروه خبرگان به ترتیب اهمیت فرضیات دوم و چهارم و سوم در کاهش کلاهبرداری اینترنتی مهم تر از نقش تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران (فرضیه چهارم) در افزایش کلاهبرداری اینترنتی، می‌باشد. همچنین از نظر خبرگان آیتم‌های آموزش و آگاه سازی کاربران اینترنت در خصوص کلاهبرداری اینترنتی (مربوط به فرضیه دوم)، آموزش کاربران در خصوص خدمات بانکداری الکترونیک توسط بانک‌ها (مربوط به فرضیه دوم)، و استفاده از نرم افزارهای امنیتی و ضد جاسوس افزارها توسط کاربران (مربوط به فرضیه چهارم) بیشترین تاثیر را در کاهش کلاهبرداری اینترنتی داشته‌اند.

نتایج به دست آمده از سمت گروه کاربران (قربانیان جرم کلاهبرداری اینترنتی)

مقدار آماره آزمون Kmo در گروه کاربران (قربانیان جرم کلاهبرداری) برابر با ۰/۸۰۱ بوده و از ۰/۸ بیشتر می‌باشد هم چنین با توجه به اینکه سطح معنی داری در این گروه ۰/۰۰۰ بوده و کمتر از ۰/۰۵ می‌باشد (sig<۰/۰۵) لذا با اطمینان ۹۵ درصد می توان گفت در گروه کاربران (قربانیان جرم کلاهبرداری) فرضیه H۱ پذیرفته شده و فرضیه H۰ رد می‌شود بنابرین بین عوامل مورد نظر و کلاهبرداری اینترنتی ارتباط معنی دار وجود دارد. و به عبارت دیگر با اطمینان ۹۵ درصد می توان گفت کلیه عوامل ذکر شده در پرسش نامه در کلاهبرداری اینترنتی موثر می‌باشد. با مقایسه میانگین سوالات مربوط به هر فرضیه این نتیجه حاصل گردید که گروه کاربران (قربانیان جرم کلاهبرداری) از خدمات مبتنی بر فناوری اطلاعات و اینترنت استفاده می‌نموده‌اند لذا از سمت کاربران تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران (سوالات ۱-۲-۳-و۴) بر

افزایش کلاهبرداری اینترنتی تاثیر داشته است. اما در صورتی که استفاده کاربران از خدمات مبتنی بر فناوری اطلاعات همراه با آگاه سازی وآموزش کاربران، انجام احراز هویت و پروسه‌های تصدیق هویت و استفاده از نرم افزارهای امنیتی باشد،آنگاه تاثیر تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در افزایش کلاهبرداری زیاد نخواهد بود.

با مقایسه ضریب بارعاملی فرضیات مطرح شده در تحقیق برای گروه کاربران (قربانیان جرم کلاهبرداری) ؛ ضرایب محاسبه شده برای عوامل تفاوت چندانی نداشته و نمی توان به صورت قطعی اولویت خاصی را مشخص نمود اما با اغماض می توان گفت بیشترین تاثیر را از بین عوامل از نظر گروه کاربران (قربانیان جرم کلاهبرداری) ؛ انجام احراز هویت و پروسه‌های تصدیق هویت داشته(فرضیه سوم) و افزایش سطح آگاهی و آموزش کاربران (فرضیه اول) در اولویت دوم ؛ استفاده از ابزارهای امنیتی (فرضیه چهارم) رتبه سوم و از نظر گروه کاربران به ترتیب اهمیت فرضیات دوم و چهارم و سوم در کاهش کلاهبرداری اینترنتی مهم تر از اهمیت تغییرات تکنولوژیک در سطح خدمات IT مورد استفاده کاربران در افزایش کلاهبرداری اینترنتی، می‌باشد. با توجه به مقایسه میانگین سوالات قربانیان می توان به صورت توصیفی نتیجه گرفت که اکثریت گروه قربانیان جرم کلاهبرداری اینترنتی در ایران از پست الکترونیک برای مبادله و ارسال و دریافت اسرار و اسناد تجاری و مالی استفاده می کنند؛همچنین اکثریت قربانیان ایمیل‌ها و لینک‌های ناشناس را باز می کنند و از سویی اکثریت پاسخ دهندگان در این گروه به نصب نرم افزارهای امنیتی هم چون ضد ویروس ؛ ضد جاسوس افزار و فایروال در سیستم‌های خود که مبادلات مالی و بانکی خود را با استفاده از آنها انجام می‌دهند توجه نمی کنند.

منابع

- اصغری، خدیجه. قلی زاده، بهروز. مدیری، ناصر(۱۳۹۲)، ارائه روشی برای بهبود احراز هویت در تجارت الکترونیک، اولین کنفرانس ملی نوآوری در مهندسی کامپیوتر و فناوری اطلاعات.
- اکبری، عباسعلی(۱۳۹۰) ،کلاهبرداری رایانه ای جلوه های نوین و متمایز از کلاهبرداری سنتی، همایش منطقه ای چالشهای جرایم رایانه ای در عصر امروز.
- امینی، محمد. جعفری، محمد جواد (۱۳۹۲) ، بررسی مقایسه ای مدلهای تشخیص تقلب در مزایده های آنلاین،اولین کنفرانس ملی نوآوری در مهندسی کامپیوتر و فناوری اطلاعات.
- باستانی، برومند(۱۳۹۰) ، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، تهران انتشارات بهتامی.
- بوربور، مسعود(۱۳۹۳)، تبیین شیوه های مبتنی بر فناوری اطلاعات برای پیشگیری از کلاهبرداری های مالی موجود در فضای مجازی، پایان نامه کارشناسی ارشد، دانشگاه علوم انتظامی.
- جعفری، مریم .سلیمانی، فرزاد (۱۳۹۴)، نقش پلیس در تأمین امنیت و سال مسازی فضای سایبر با رویکرد پیشگیری اجتماعی از جرایم سایبری، همایش ملی سبک زندگی، نظم و امنیت.
- حسن زاده، محبوبه (۱۳۹۲)، جرایم رایانه ای و راهکارهای پیشگیری و مبارزه با آن، اولین کنفرانس ملی نوآوری در مهندسی کامپیوتر و فناوری اطلاعات.
- ذبیحی، سلمان (۱۳۹۱)، تبیین چگونگی تأثیر جرایم رایانه ای بر امنیت ملی کشور، پایان نامه کارشناسی ارشد، دانشگاه قم.
- رجبی پور، محمود (۱۳۹۳)، درآمدی بر پیشگیری مقتدرانه پلیس از جرم، فصلنامه دانش انتظامی، سال ششم، شماره دوم.
- زلف پور، مرتضی. مرادی، محسن. مرادی، مهرداد. امیدوار، محمدنبی (۱۳۹۴)، رتبه بندی آنتی ویروس ها با استفاده از روش تصمیم گیری چند معیاره، دومین همایش ملی ریاضیات و کاربردهای آن در علوم مهندسی.
- ساعدی، پریا (۱۳۹۲)، بررسی راهکارهای پیشگیری اجتماعی از کلاهبرداری سایبری، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران شمال.

- سالارزهی، حبیب . جمشیدی، محمدجواد . جمشیدی، محمد جعفر (۱۳۹۰)، مدل پیشنهادی مقابله با جرایم رایانه ای، همایش منطقه ای چالش های رایانه ای در عصر امروز.
- صدوقی، مجید(۱۳۹۲). پژوهش کیفی در روان شناسی و علوم رفتاری، انتشارات هستی نما، تهران.
- غروی، عرفانه. محمدی شهریار(۱۳۹۲)، کاربرد تکنیکهای داده کاوی جهت تشخیص آدرسهای فیشینگ، کنگره ملی مهندسی برق، کامپیوتر و فناوری اطلاعات.
- کاظمی شریعت پناهی، سید حسن (۱۳۹۲)، آگاهی از انواع جرایم اینترنتی و راهکارهای پیشگیری و یا مقابله با آنها: با تأکیدی بر انواع و نمونه های سرقت هویت، نخستین همایش منطقه ای فناوری اطلاعات.
- مشرقی کاشانی، نرگس. خلیلی، مهدی (۱۳۹۳)، تدوین مدل چند سطحی برای کشف کلاهبرداری در پرداختهای الکترونیکی، اولین کنفرانس ملی چالش های مدیریت فناوری اطلاعات در سازمان ها و صنایع.
- هدایتی، حمید. عبدلی، غلامرضا (۱۳۹۳)، تکنولوژی تجارت الکترونیک و پیدایش جرائم نوین، کنگره ملی پژوهش های کاربردی علوم انسانی اسلامی.
- هفت تنی، علی اصغر. المیرا امسیا، محبوبه درخشنده (۱۳۹۳)، نقش رسانه در پیشگیری از جرایم سازمان یافته، اولین کنفرانس بین المللی اقتصاد، مدیریت، حسابداری و علوم اجتماعی.
- هوارد، ریچ. مترجم بهزاد لک (۱۳۹۴)، کلاهبرداری سایبری: تاکتیک ها، تکنیک ها و رویه ها، تهران انتشارات دانشگاه علوم انتظامی.
- Aaron Schwabach" (2014) Internet And The Law Second Edition" Publisher: ABC-CLIO
- Adam Levin, Beau Friedlander2015 "Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves "Publisher: PublicAffairs,
- Ajeet Singh Poonia, Awadesh Bhardwaj, G. S. Dangayach" 2011 Cyber Crime: Practices and Policies for Its Prevention" The First

International Conference on Interdisciplinary Research and Development,

- Anthony Abayomi Adebayo" 2013 Social Factors Affecting Effective Crime Prevention and Control in Nigeria" International Journal of Applied Sociology,
- Askerniya Imran, Hamid Jahankhani, Sin Wee Lee" 2012Education, Training and Awareness (ETA) Four Dimensional cybercrime prevention model" Kaspersky
- Collins, Brian S. and Mansell, Robin2014 "Cyber trust and crime prevention" Trust and crime in information societies. Edward Elgar, Cheltenham, UK, pp. 58-11. ISBN 1845421779
- Dunn, John E.2014 "Ransom Trojans spreading beyond Russian heartland". TechWorld.
- EK Rotich, SK Metto, GM Muketha" 2014.A survey on cybercrime perpetration and prevention: A review and model for CyberCrime prevention" European Journal of Science and Engineering,
- European Banking Authority2014 "EBA Opinion on 'virtual currencies". 4 July 2014. p. 46.
- Fasanmi, Samuel Sunday , Kaburuk, Daniel Sarah ,Ariyo, Adenike Bosede"2014 Influence of Psycho-social Factors on Youths' Attitude towardsInternet Fraud in Nigeria" 4th world Conference on Educational Technology Researches.
- James Byrne and Gary Marx"2013 Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact" International Journal of Applied Sociology
- Katie A. Farina"2015 Cyber Crime: Identity Theft" International Encyclopedia of the Social & Behavioral Sciences (Second Edition),

Pages 637–633

- M Lakshmi Prasanthi"2015 Cyber Crime: Prevention & Detection" International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 3,
- Mohini Singh & Margaret Jackson"2015 Online Dating Sites: A tool for romance scams or a lucrative e-business model? "28th Bled eConference
- Rajarshi Chakraborty, Jaeung Lee, Sharmistha Bagchi-Sen, Shambhu Upadhyaya" 2016 Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults" Decision Support Systems, Available online .
- Sidney Tsang, Yun Sing Koh, Gillian Dobbie"2015 Finding collaborative frauds in online auctions" International Conference on Computer, Communication and Convergence,
- Soudabeh Vahdati, 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, Volume 51, Part A, Pages 187–180
- Steve Watts,2016 Secure authentication is the only solution for vulnerable public wifi, Computer Fraud & Security, Volume 2016, Issue 1Pages 20–18