

عناصر متشکله جرم کلاهبرداری در فضای مجازی با مطالعه نظام حقوق کیفری ایران

کتایون بلالائی صومعه سرائی

کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه علوم و تحقیقات رشت، گیلان، ایران

Hoghogh.law71@gmail.com

چکیده :

امروزه از کلاهبرداری رایانه‌ای می‌توان به لحاظ دسترسی سریع و سهولت ارتکاب جرم، شایع‌ترین جرم اقتصادی در فضای مجازی و رایانه نام برد. کلاهبرداری رایانه‌ای در قوانین کیفری ایران، به لحاظ ارکان مادی و معنوی با کلاهبرداری سنتی (موضوع ماده ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری) تفاوت‌هایی داشته و هرکدام ویژگی‌های خاص خود را دارد. اگر بخواهیم به معنای کلاهبرداری در فضای مجازی نگاهی بیندازیم متوجه می‌شویم که محل وقوع جرم فضای مجازی و سیستم‌های رایانه‌ای و مخابراتی است که فرد کلاهبردار با استفاده از ابزار و روش‌های متقلبانه و یا حتی بدون فریب دادن بزه دیده و عدم آگاهی او مرتکب جرم کلاهبرداری شده است و از این طریق اموال وی را در اختیار خود قرار داده و تصاحب می‌نماید حال ممکن است از طریق حساب‌های بانکی، اطلاعات هویتی و یا شبکه‌های اجتماعی باشد. در گذشته کلاهبرداری به روش سنتی به کرات دیده می‌شد که کلاهبردار با توسل به وسایل متقلبانه موجب می‌شد که بزه دیده با رضایت خود و بدون هیچ‌گونه اجبار و تهدیدی اموال خود را اعم از منقول و یا غیر منقول هم چنین اسنادی هم چون چک، سفته و یا هر سند دیگری را در اختیار کلاهبردار قرار دهد. هدف از انتخاب این موضوع آگاهی جامعه در مورد یکسری جرائم که به ظاهر ممکن است نوعی جرم به شمار نیایند و به صورت غیرقابل ملموس در محیط‌های مجازی صورت گیرد می‌باشد. آنچه مسلم است کلاهبرداری در فضای مجازی با منفعت، خدمات و امتیازات مالی بزه دیده سر و کار دارد بدین صورت که قصد تحصیل مال غیر و ورود ضرر و زیان مادی به بزه‌دیده وجود داشته باشد. در این مقاله سعی شده است که به ابعاد و اجزای تشکیل دهنده ی جرم کلاهبرداری در فضای مجازی و روش‌های ارتکاب این جرم بپردازیم.

کلید واژه : فضای مجازی، جرم، بزه دیده، کلاهبرداری

مقدمه :

امروزه فضای سایبر جایگزین واژه فضای مجازی شده است که در رسانه‌ها و دنیای ارتباطات شنیده می‌شود و به این صورت تعریف می‌شود: وارد کردن، تغییر، محو یا موقوف‌سازی داده‌های کامپیوتری یا مداخلات دیگر در داده‌ها که بر نتیجه پردازش آنها اثر گذاشته و به قصد تحصیل خدمات و امتیازات اقتصادی غیر مجاز موجب خسارات اقتصادی خواهد شد. این فضای جدید به گونه‌ای کلاهبرداری سنتی را دچار تحولات اساسی نموده به طوری که تعریف این جرم در فضای مجازی با تعریف اصل کلاهبرداری منطبق نبوده و در اکثریت موارد متفاوت عمل کرده است (حسن بیگی، ۱۳۸۴) کلاهبرداری رایانه‌ای امروزه یکی از مهم‌ترین جرائم ناشی از سوء استفاده از فناوری اطلاعات به شمار می‌آید و روز به روز در حال افزایش است با توجه به حضور کاربران در فضای اینترنتی و پیشرفت‌های علم الکترونیک در جهان می‌توان به آن پی برد در واقع پیدایش رایانه و فراگیری سریع فناوری اطلاعات زمینه‌هایی را ایجاد نمود که کاربر بدون نیاز به برنامه نویسی و هیچ‌گونه خلاقیتی مرتکب جرائم اینترنتی شود در واقع فضای مجازی مکان مناسبی را برای بزهکار فراهم می‌نماید (علی نژادی، ۱۳۹۷) کلاهبرداری رایانه‌ای یکی از انواع مهم و معمول جرم کلاهبرداری در چند سال اخیر است طبق ماده ۷۴۱ قانون مجازات اسلامی

(ماده ۱۳ قانون جرایم رایانه ای) اگر فرد با استفاده از رایانه اقدام به محو، توقف، تغییر، ورود یا ایجاد اختلال غیر مجاز در یک سامانه شده و مالی را جابجا کرده یا داده ها و اطلاعاتی را سرقت نماید و به وسیله آنها بتواند امتیاز مالی یا وجهی را از قربانی برباید مرتکب جرم کلاهبرداری رایانه ای شده و مجازات قابل توجهی برای وی در نظر گرفته می شود هم چنین ساخت و استفاده از صفحات فیشینگ (صفحات پرداخت بانکی) و ساخت برنامه و نرم افزارها یا نگارش هر گونه محتوای دیجیتال برای دسترسی به اطلاعات مالی افراد جزء کلاهبرداری اینترنتی هستند.

تعریف جرم کلاهبرداری رایانه ای :

رفتار مرتکب در جرم کلاهبرداری در فضای مجازی تنها به صورت فعل مثبت محقق می شود. قانون به طور خاص در کنار قوانین عمومی حاکم بر کلاهبرداری یک عنوان مجرمانه مستقل یعنی کلاهبرداری رایانه ای پیش بینی کرده است که یکی از جرایم متداول در ایران است و بیشترین جرم در بین جرایم سایبری مربوط به کلاهبرداری اینترنتی می باشد و تمام مصادیق جرم کلاهبرداری را نیز در بر می گیرد که در ماده ۱۳ قانون جرایم رایانه ای ذکر شده است (زراعت، ۱۳۹۲) اقداماتی از قبیل وارد کردن تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه، که قانونگذار از عبارت از قبیل استفاده کرده است بنابراین عناوین به کار رفته جنبه تمثیلی دارند و ممکن است این جرم به صورت های دیگری نیز واقع شود. نکته ی دیگر این است که ارتکاب این اعمال باید به تحصیل وجه، مال و یا خدمات و امتیازات مالی برای خود یا دیگری بینجامد تا بتوانیم بگوییم شخص مرتکب جرم کلاهبرداری رایانه ای شده است و باید نتیجه محقق شود در غیر اینصورت عمل مشمول عنوان مجرمانه دیگری مانند تخریب یا اختلال در داده ها و دیگر عناوین خواهد بود و برخلاف کلاهبرداری سنتی که فقط گرفتن مال دیگری با توسل متقلبانه را شامل می شود کلاهبرداری در فضای رایانه علاوه بر مال امتیازات مالی و یا خدمات و هم چنین تحصیل منفعت را در خود گنجانده است. در کلاهبرداری رایانه ای انسان فریب نمی خورد بلکه اصطلاحاً سامانه رایانه ای فریب می خورد (زیبر، ۱۳۹۰) ماده فوق الذکر در مقایسه با ماده یک قانون تشدید مجازات مرتکبین ارتشا اختلاس و کلاهبرداری که به تعریف کلاهبرداری ساده پرداخته مجازات متمایزی دارد و هم چنین تعاریف متفاوتی با یکدیگر دارند. در واقع کلاهبرداری رایانه ای سامانه ها یا سیستم پردازش داده هدف قرار می گیرند در واقع انسان با یک سامانه رایانه ای و مخابراتی روبرو خواهد بود اما در کلاهبرداری موضوع ماده یک قانون تشدید مرتکب سعی بر تاثیر گذاری بر بزه دیده دارد البته لازم به ذکر است کلاهبرداری سنتی ممکن است در فضای مجازی و از طریق رایانه رخ دهد در واقع رایانه به عنوان یک وسیله برای فریب کاربر و انجام اعمال متقلبانه مورد استفاده قرار گیرد و نباید این رفتار را کلاهبرداری رایانه ای دانست (آقایی نیا و رستمی، ۱۳۹۷) زیرا در این جا رابطه مستقیم بین کلاهبردار و شخص مالباخته در فضای مجازی وجود دارد و شخص مالباخته با رضایت کامل وجه را از این طریق به حساب کلاهبردار واریز می نماید اگر چه ما نمی توانیم تعریف کلاهبرداری سنتی را در این قانون یا دیگر قوانین جزایی مشاهده کنیم اما با نگاه به متن ماده یک قانون تشدید مجازات مرتکبین ارتشا اختلاس و کلاهبرداری و مصادیق مندرج در متن در می یابیم که این تعریف براساس تعریف فقها از کلاهبرداری بوده و بر همین اساس می توان گفت: «کلاهبرداری یعنی بردن مال دیگری از طریق توسل همراه با سوء نیت به وسایل یا عملیات متقلبانه» (میرمحمد صادقی، ۱۳۸۶)

به طور کلی رفتارهای فیزیکی لازم جهت شکل گیری کلاهبرداری رایانه ای به دو قسمت تقسیم می شود. قسمت اول مصادیق ماده ۱۳ قانون جرایم رایانه ای می باشد که منحصرأ با فعل مثبت محقق می شود و این حالت برای تمام موارد موضوع ماده ۱۳ بوده و تمثیلی است در نتیجه تنها رفتارهای مشابه و مرتبطی که با فعل مثبت محقق می شود را مشمول این ماده باید دانست. قسمت دوم تحصیل غیرمجاز موضوع این جرم است که شامل وجه، مال، منفعت، خدمات و یا امتیازات مالی می باشد. یکی از این مصادیق وارد کردن داده ها می باشد که به هر نحوی منجر به موضوع این جرم می گردد را کلاهبرداری رایانه ای دانسته است. به عنوان مثال اگر شخصی کارت بانکی خود را جهت گرفتن موجودی به دیگری بدهد و فرد وجهی از آن حساب را برای

خود بردارد مشمول کلاهبرداری رایانه ای است ، هر چند با رضایت شخص صورت گرفته اما در نهایت شروع به وارد کردن داده ها نموده و به نفع خود وجه را تصاحب کرده است. (بابایی ، ۱۳۹۷)

شرایط لازم جهت تحقق کلاهبرداری رایانه ای :

شرط اول تحقق جرم این است که اموال متعلق به خود نباشد و متعلق به شخص دیگری باشد یعنی اگر اموال برای خود مرتکب باشد کلاهبرداری محقق نخواهد شد. شرط دوم و اساسی برای ارتکاب جرم کلاهبرداری رایانه ای مصادیق تمثیلی ماده ۱۳ مذکور و هم چنین ضرر حاصله از این اقدامات می باشد که از طریق سیستم های رایانه ای رخ می دهد پرداخته است که در زمان ارتکاب جرم احتیاج مستقیم به داده ها و سامانه های رایانه ای وجود دارد بر این اساس چنین مواردی از شمول ماده یک قانون تشدید خارج شده است و عنوان کلاهبرداری با شرایط خاصی منصرف به حقوق کیفری ایران است و در کلاهبرداری در همه مصادیق فریب قربانی شرط به وقوع پیوستن جرم نیست (سالاری ، ۱۳۹۳)

امروزه کلاهبرداری اینترنتی از کلاهبرداری سنتی پیش گرفته و بر پیچیدگی های این نوع جرایم می افزاید هر چند قوانین در این زمینه ها جامعیت کافی را نخواهد داشت و به همین دلیل مجرمین راه حل های فرار از قوانین را به سرعت پیدا می کنند کلاهبرداری رایانه ای تفاوتی با جرم کلاهبرداری سنتی ندارد و تنها شیوه آن متفاوت تر شده است .

جرم کلاهبرداری رایانه ای به لحاظ رکن مادی در زمره جرائم مطلق است و ضرورتی به فریب بزه دیده ، بردن مال ، ورود ضرر یا انتفاع مرتکب نیست اما مقید به حصول نتیجه مجرمانه است یعنی باید به واسطه سوء استفاده از سیستم های رایانه و مخابراتی از طریق افعالی نظیر ایجاد ، محو ، توقف داده ها و غیره مال یا منفعت یا مزایای مالی عاید مرتکب جرم گردد . کلاهبرداری را جرم مرکب می دانیم زیرا از دو یا چند رفتار فیزیکی تشکیل شده است و نتیجتاً بردن مال در فضای رایانه ای و یا تحصیل خدمات و امتیازات مالی حتی در جایی که کلاهبردار به بزه دیده می گوید که پول را به حسابش واریز نماید به محض واریز شدن کلاهبرداری انجام شده با این که کلاهبردار هنوز به بانک نرفته و وجه را دریافت نکرده است . زیرا واریز شدن به حساب همان بردن مال دیگری به طور اعتباری است و هم چنان جرم کلاهبرداری رایانه ای را جرم مرکب می دانیم (عالی پور ، ۱۳۹۳) رفتار فیزیکی کلاهبرداری در فضای مجازی سوء استفاده یا استفاده غیر مجاز از داده های پیام است ولیکن این رفتار می تواند در قالب افعال تمثیلی نظیر ورود ، محو ، توقف داده پیام و ... متجلی شود و فضای سایبر که کاربران در آن برای همدیگر ناشناخته هستند به نظر می رسد فریب دیگران در این جرم لازم نباشد و هدف رایانه و نرم افزارهای آن می باشد و کمتر در این فضا بحث قربانی پیش می آید. (خرم آبادی ، ۱۳۸۶)

عناصر تشکیل دهنده جرم کلاهبرداری :

هر جرمی دارای عناصر تشکیل دهنده است این عناصر تشکیل دهنده شامل عنصر قانونی ، مادی و معنوی می باشد . عنصر قانونی جرم کلاهبرداری رایانه ای همان تعریف قانونی ماده ۱۳ قانون جرایم رایانه ای است. مطابق ماده ۷۴۱ قانون مجازات اسلامی (ماده ۱۳ فوق الذکر) که به واسطه آن فعل یا انجام ندادن عملی جرم شناخته می شود . عنصر قانونی جرم کلاهبرداری رایانه ای در بستر مبادلات غیر الکترونیکی ساده است هم جرم و هم مجازات در یک ماده قانونی آمده است . نمونه کلاهبرداری رایانه ای در بستر غیر مبادلات الکترونیکی مانند این است که مرتکب با ارسال پیام مبنی بر برنده شدن غیر واقعی شخصی برای بردن یک دستگاه ماشین و واریز مقداری وجه در قبال تحویل جایزه مالباخته با انتقال وجه به حساب کلاهبردار دیگر خبری از جایزه نباشد عنصر مادی جرم کلاهبرداری عبارتست از هر گونه کنش مرتبط با داده یا سامانه گفته می شود مانند : محو کردن ، ایجاد ، متوقف کردن یا مختل کردن سامانه و غیره که باید به صورت غیر مجاز انجام گیرد .

در واقع رایانه وسیله ی ارتکاب جرم کلاهبرداری رایانه ای است و نقش اساسی در ارتکاب این جرم دارد . دوم تحصیل اعم است از دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خود (جعفری لنگرودی ، ۱۳۸۸) در جرم کلاهبرداری رایانه ای مرتکب از طریق دادن برنامه ای بدون مجوز و مخفیانه به رایانه ، موفق به تحصیل وجوه یا اموال از بانک یا شرکت یا یک

مؤسسه مالی می گردد به عنوان مثال اگر کسی به سامانه بانک وارد شود و با دگرگونی داده ها یعنی تغییر یا تبدیل داده ها ، رقم پولی دارنده حسابی را کاهش و رقم حساب خود را افزایش دهد مرتکب کلاهبرداری رایانه ای شده است و یا با وارد کردن به سامانه یک مؤسسه مالی ، درصد اقساط وامی که باید برگردانده شود را کاهش دهد یا با دستکاری در سامانه برخی از اقساط وام را پرداخت شده نشان دهد فاعل جرم کلاهبرداری رایانه ای است سوم موضوع کلاهبرداری رایانه ای وجه ، مال منفعت ، خدمات یا امتیازات مالی است که اقدامات موضوع ماده ۱۳ قانون جرایم رایانه ای مانند وارد کردن داده ها تغییر ، محو و غیره به خودی خود کلاهبرداری نبوده و آخرین فرایند رکن مادی (بردن مال ، امتیاز ، منفعت و یا خدمات مالی) باید تحقق پیدا کند (باستانی ، ۱۳۹۰) کلاهبرداری در فضای رایانه ای عبارتست از اقدامات و دخالت غیر مجاز در رایانه که شامل مصادیق زیر است :

الف (وارد کردن داده ها : مرتکب با وارد کردن داده ها و اطلاعات مالی ، وجه یا امتیاز تحصیل می نماید . در این رابطه آن چه اهمیت دارد غیر مجاز بودن رفتار مرتکب در وارد کردن داده است . حال ممکن است از طریق صفحه کلیدها و یا دیگر ابزارهای ورودی رایانه باشد و مرتکب بدون اجازه و رضایت شخص صاحب حساب به اطلاعات او دست می یابد و قصد جعل از طرف مرتکب وجود ندارد . ظاهراً منظور از استفاده از داده ها ، داده های جعلی می باشد نه داده های مجاز اما ماده ۷۴۱ قانون مجازات اسلامی مطلق بوده و تفاوتی بین نوع داده ها قائل نشده است (نظریه مشورتی اداره حقوقی قوه قضائیه ، ۱۳۹۳) به طور کلی وارد کردن داده ها به دو حالت قابل تحقق است یکی وارد کردن داده های غیر صحیح و غیر مجاز و دیگری وارد کردن غیر مجاز داده های صحیح ، نظریه مشورتی نیز تقویت کننده این استدلال است از موارد مبتلا به این مصداق از جرم کلاهبرداری رایانه ای هک کردن اطلاعات حساب بانکی افراد است که برخی از افراد تحت تأثیر تبلیغات مجازی و سایت های جعلی در شبکه های اجتماعی قرار گرفته و سود جویان اطلاعات کارت بانکی آنها را به طور غیر مجاز دریافت می کنند و مبلغی را برداشت می نمایند .

ب (تغییر داده ها : چنانچه جعل رایانه ای مصداق تغییر غیر مجاز داده ها قرار گیرد و این تغییر داده منتج به تحصیل مال ، وجه یا امتیاز گردد جرم کلاهبرداری رایانه ای واقع شده است .

ج (محو داده ها : شامل از بین بردن و حذف داده ها است در صورتی که این محو در جهت تحصیل وجه یا امتیازات مالی باشد می تواند از مصادیق کلاهبرداری رایانه ای باشد . نفوذ به سامانه رایانه ای و مخابراتی دیگری که با تدابیر امنیتی حفاظت شده باشد با این که دسترسی غیر مجاز به داده های دیگری محسوب می شود اما برای این اقدام محو و هک شدن داده ها ضروری است . (عالی پور ، ۱۳۹۵)

د (توقف داده ها و اطلاعات رایانه ای : توقف داده ها مانند متوقف ساختن دستور پرداخت وجه به شخص و طرف پرداخت قرار دادن خود به طور غیر مجاز. متوقف ساختن داده ها ممکن است به طور دائمی یا موقت انجام گیرد. ایجاد وقفه پردازش جزئی یا کلی داده از هر طریق به منظور دستیابی به سامانه رایانه ای را متوقف کردن داده ها گویند . عمل اضافه کردن به داده های ورودی یا افزایش مقادیر ورودی را اصطلاحاً ایجاد داده گویند . (ترکی ، ۱۳۸۹)

هـ) اختلال در سامانه :

خارج کردن تمام یا قسمتی از سامانه یا سیستم از برنامه و نظم همیشگی خود به جهت رسیدن به موارد پنج گانه مزبور را مختل کردن سامانه گویند این اقدام شامل هر نوع دستکاری سخت افزارها ، جلوگیری از خروج داده ها تأثیر گذاشتن بر ثبت و ذخیره یا جریان داده ها یا توانایی اجرای برنامه ها می باشد به گونه ای که ناتوانی در وضعیت سامانه و ایجاد آشفتگی در وضعیت سامانه باعث شود سامانه پردازش صحیح خود را از دست بدهد و دسترسی به داده ها را برای کاربر به تأخیر بیندازد و متضرر از اقدام کلاهبردار گردد . هدف از مداخله در کارکرد سیستم رایانه و ایجاد اختلال غیر قانونی تحصیل مال یا وجه یا امتیاز



خدمات خواهد بود. مثلاً فردی با اختلال در سامانه ثبت تخلفات راهنمایی و رانندگی موجب حذف پیشینه تخلفات رانندگی خود گردد (صنعتی و عطایی جنتی، ۱۳۹۷)

عنصر معنوی جرم کلاهبرداری رایانه ای عبارتست از رفتار مرتکب کلاهبرداری رایانه ای باید همراه با قصد فریب دیگری یا سبب اختلال و گمراهی سیستم های پردازش خودکار و نظایر آن شود. عنصر معنوی این جرم متشکل از دو جزء قصد فعل (عمد در رفتار) و آگاهی به اجزای رکن مادی به ویژه مصادیق مندرج در ماده مربوط به جرم کلاهبرداری رایانه ای می باشد. عمد عام یعنی علم به موضوع که بحث مشترک در تمام جرایم مالی است و شرط است مرتکب بداند موضوع جرم مال غیر است و به دیگر اجزای کلاهبرداری آگاه باشد (قیاسی، ۱۳۹۳) عمد عام در واقع سوء استفاده یا استفاده غیر مجاز از داده پیام ها، برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور است که با ارتکاب افعال موضوع ۱۳ قانون جرایم رایانه ای دیگران را فریب دهد یا سبب گمراهی سیستم های پردازش خودکار و نظایر آن شود جهل یا اشتباه نسبت به موضوع جرم رکن معنوی را زائل می کند. به عنوان مثال کارمند بانک از طریق سامانه رایانه ای به اشتباه وجهی را به حساب دیگری واریز نماید به دلیل عدم علم به تعلق مال غیر رکن مادی وجود دارد اما فاقد رکن معنوی است. عمد خاص که قصد تحصیل اموال یا امتیازات مالی و بردن اموال دیگران می باشد. قصد فعل باید به شمار رفتارهایی باشد که برای تحقق جرم لازم است پس قصد فعل پیرو فعلی است که از فرایند تکوین این جرم قرار می گیرد قصد تقلب با ارتکاب آگاهانه و ارادی رفتارهایی مانند وارد کردن، محو و غیره همراه خواهد بود پدیده مجرمانه را رقم می زند و بدون وجود آن جرمی پدید نمی آید. (الهی منش و مرادی اوجقاز، ۱۳۹۵)

همانطور که اشاره شد افزون بر علم به موضوع، مرتکب باید به متقلبانه بودن رفتار خویش نیز آگاه باشد بدین معنا که شخص اراده در توسل به وسایل یا عملیات متقلبانه داشته باشد و بردن مال غیر نیز آزادانه انجام می گیرد. قصد تحصیل باید مقدم بر رکن مادی باشد در غیر این صورت به علت تقارن رکن مادی و معنوی ارتکاب جرم کلاهبرداری منتفی خواهد بود در قوانین بین المللی کلاهبرداری اینترنتی به صرف ایراد ضربه به قصد به دست آوردن منافع مالی محقق می شود. (نامور، ۱۳۹۱)

می توان نتیجه گرفت رکن معنوی یا سوء نیت در جرم کلاهبرداری رایانه ای متشکل از چند جزء است: (۱) علم مرتکب جرم به متقلبانه بودن اقدامات خود و جرم بودن عمل و قصد ضرر زدن به مالباخته (۲) سوء نیت عام (۳) سوء نیت خاص و باید خاطر نشان کرد که انگیزه مرتکب تاثیری در ارتکاب این جرم ندارد.

روش های ارتکاب جرم کلاهبرداری رایانه ای :

به طور کلی روش های ارتکاب جرم کلاهبرداری رایانه ای متفاوت است که به متداول ترین آنها اشاره می نمایم .
کلاهبرداری اینترنتی و فروش آنلاین:

امروزه با توجه به گسترش روابط افراد و افزایش روزافزون استفاده افراد جامعه از اینترنت اکثر جرایم مالی از حالت سنتی خود خارج شده اند جرم کلاهبرداری نیز از آن قاعده مستثنی نیست. بسیاری از کلاهبرداران با سوءاستفاده از فضای اینترنت و اعتماد مردم عملیات متقلبانه خود را در فضای مجازی مرتکب می شوند با روی آوردن بسیاری از مردم جهت استفاده از خدمات اینترنتی و خریدهای آنلاین جرایم این حوزه متأسفانه رو به افزایش است در این نوع کلاهبرداری مرتکب فروشگاه مجازی راه اندازی می کند و ادعای فروش محصولاتی دارد و شخص مال باخته بدون اطلاع از وضعیت این فروشگاه اینترنتی اقدام به خرید و پرداخت وجه می نماید .

کلاهبرداری بازاریابی شبکه ای :

مرتکبین این نوع کلاهبرداری غالباً شرکت های هرمی می باشند به این صورت که افراد به خرید و فروش محصولات مصرفی می پردازند و از طریق اخذ پورسانت یا عضوگیری کسب در آمد می نمایند در حال حاضر بسیاری از شرکت ها تنها از راه

عضوگیری کسب در آمد مینمایند و در واقع محصولی را به فروش نمی رسانند و افرادی را که در راس این شرکت ها هستند از عضوایی دیگران سودهای کلان به جیب می زنند .

کلاهبرداری از نوع خالی کردن حساب به بهانه قرعه کشی :

در این روش کلاهبرداران شماره تماس مشتریان را در سایت ها به بهانه قرعه کشی جمع آوری می کنند و با آنها تماس می گیرند یا پیامک هایی مبتنی بر شما برنده شده اید ارسال می نمایند و از کاربران می خواهند تا مبلغی را برای ارسال جازه واریز نمایند این دسته از کلاهبرداری ها در مواردی فقط واریز هزینه ارسال هستند اما در مواردی حاوی لینک درگاه جعلی هستند با که این روش قدیمی است اما هم چنان افراد زیادی را در دام می اندازد .

کلاهبرداری پیامکی :

این روش استفاده از سامانه های پیامکی است و هم چنین ارسال انبوه پیامک است اصولاً این افراد با ارسال پیامک هایی به عنوان مثال شما برنده جایزه شدهاید وارد لینک زیر شوید به محض ورود شخص و کلیک پیامک ارسالی مرتکب به اطلاعات گوشی شخص دسترسی پیدا می کند و حسابشان را خالی می نمایند .

فیشینگ (درگاه پرداخت اینترنتی جعلی) :

در این روش کلاهبرداران صفحه درگاهی کاملاً مشابه درگاه پرداخت های واقعی می سازند و اطلاعات حساب یعنی شماره کارت و غیره را ذخیره می نمایند و حساب بانکی افراد را خالی می نمایند. کلاهبرداران در این روش برای جلوگیری از ایجاد شک در ذهن کاربران پس از دریافت تمامی اطلاعات کارت از جمله رمز کارت پیغام خطا در اتصال به بانک یا عدم انجام تراکنش را نشان می دهند .

کلاهبرداری از طریق سرقت اطلاعات هویتی :

این روش حيله و تقلب در رابطه با هویت یک شخص دیگر است تا مرتکب از طریق آن هویت منافع یا مالی به دست آورد و به دلیل استفاده از ابزار متقلبانه با جرم سرقت اینترنتی متفاوت است و به نظر می رسد بهتر بود از عبارت سرقت هویت استفاده نمی شد و عنوان کلاهبرداری هویت عنوان میشد (میر محمد صادقی، ۱۳۹۵)

در این روش پیامک یا ایمیل حاوی لینک پرداخت برای افراد ارسال می کنند و کاربران بر روی این لینک ها به درگاه های جعلی (فیشینگ) منتقل و اطلاعات آنها سرقت می شود و در واقع از افراد برای این اقدام اطلاعات هویتی شان درخواست می شود .

مجازات جرم کلاهبرداری رایانه ای :

طبق ماده ۷۴۱ قانون مجازات اسلامی (ماده ۱۳ قانون جرایم رایانه ای) مجازات مرتکب این نوع جرایم علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هردو محکوم خواهد شد . به نظر می رسد این ماده اشخاص حقیقی را صرفاً شامل می شود زیرا از واژه هرکس استفاده نموده است . طبق نظر و صلاحدید دادگاه اگر جرمی که اتفاق افتاده جز مصادیق مجرمانه در ماده فوق الذکر باشد طبق قانون مجازات مختلفی برای مجرم در نظر خواهد گرفت. در وهله اول مرتکب ملزم است هر نوع مال ربوده شده را به شخص مال باخته مسترد نمایند و مجازات های دیگر در نظر گرفته شده یک تا پنج سال حبس یا پرداخت جزای نقدی بین دو تا ده میلیون تومان است. هم چنین دادگاه می تواند طبق صلاحدید خود مجرم را به هر دو مجازات حبس و جزای نقدی محکوم نماید. در رابطه با رد مال در پرونده های کلاهبرداری رضایت شاکی می تواند باعث تخفیف در مجازات یا حتی مختومه شدن پرونده و گذشت از مجازات متهم شود. هم چنین طبق ماده ۶۷ قانون تجارت الکترونیک مجازات جرم کلاهبرداری کامپیوتری در بستر مبادلات الکترونیکی رد مال به صاحب اموال ، حبس از یک تا سه سال پرداخت جزای نقدی معادل مال مأخوذه خواهد بود . در حالی که مجازات کلاهبرداری سنتی موضوع ماده یک قانون تشدید مجازات مرتکبین ارتشا اختلاس و کلاهبرداری یک تا هفت سال حبس و جزای نقدی معادل مالی که

اخذ نموده می باشد مجازات کلاهبرداری رایانه ای تقریباً شبیه کلاهبرداری سنتی می باشد در کلاهبرداری سنتی مجازات در نظر گرفته شده برای مجرمی است که با حيله و تقلب مال دیگری را ببرد اما کلاهبرداری رایانه ای علاوه بر مال منفعت و خدمات و امتیازات را نیز اشاره داشته است و این یک امتیاز برای کلاهبرداری رایانه ای نسبت به کلاهبرداری سنتی در قانون تشدید محسوب می شود و مصادیق مختلفی از تمامی وسایل مرتبط با رایانه و مخابرات را در بر می گیرد .

نتیجه گیری

در جرم کلاهبرداری رایانه ای اغفال و فریب بزه دیده شرط نیست و بردن مال غیر بخشی از رفتار مرتکب برای ارتکاب این جرم است و نتیجه حاصل از جرم محسوب نمی شود جرم کلاهبرداری اینترنتی معمولاً با اطلاع قبلی و رضایت بزه دیده صورت می گیرد البته ممکن است فرد بر اثر بی اطلاعی هم قربانی این جرم شود از طریق سامانه رایانه ای و مخابراتی اطلاعات شخصی او دستکاری شود. شرایط لازم جهت محقق شدن جرم کلاهبرداری رایانه ای نیازمندی مستقیم به سامانه رایانه ای و مخابراتی و هم چنین تعلق مال به غیر می باشد کلاهبرداری رایانه ای همانطور که در متن مقاله تشریح شد بر خلاف برداشت عام و رایج یک جرم مطلق بوده و بخشی از فرایند رکن مادی محسوب می شود و به صرف تحصیل جرم واقع می شود و نتیجه در آن شرط نیست و همین که مال در سلطه کلاهبردار قرار گیرد کافی است. طبق ماده ۱۳ قانون جرایم رایانه ای مقنن به ذکر افعالی همچون تغییر، محو و وارد کردن و متوقف کردن داده ها و غیره اشاره نموده و انجام این افعال در فضای اینترنت را اگر برای فریب و به دست آوردن اطلاعات و یا پول باشد جرم انگاری کرده است .

مراجع

- الهی منش ، محمد رضا و محسن مرادی اوجقاز، جرایم علیه اموال و مالکیت ، چاپ چهارم ، تهران ، انتشارات مجد، ۱۳۹۵
- باستانی ، برومند ، جرائم کامپوتری و اینترنتی ، جلوه ای نوین از بزهکاری ، چاپ سوم تهران ۱۳۹۰
- نامور، اسماعیل، ارکان تشکیل دهنده بزه کلاهبرداری در حقوق کیفری ایران و فرانسه، فصلنامه تخصصی حقوق ۱۳۹۱
- صنعتی ، سید مهدی و مجید عطایی جنتی، تحلیلی بر جرایم رایانه ای و مخابراتی (جرایم در بستر رایانه، فضای مجازی و شبکه های اجتماعی و پیام رسان ها) قم، حقوق پویا ۱۳۹۷
- عالی پور ، حسن ، حقوق کیفری فناوری اطلاعات ، چاپ چهارم تهران تهران خرسندی ۱۳۹۵
- قیاسی ، جلال الدین و عباسعلی نیک نسب ، تحصیل متقلبانه خدمات، پژوهش نامه حقوق کیفری ، سال پنجم شماره ۲، پاییز و زمستان ۱۳۹۳
- زبیر، اولدیش، جرایم رایانه ای ، ترجمه محمد علی نوری ، رضا نخجوانی ، چاپ دوم ، تهران ، کتابخانه گنج دانش ۱۳۹۰
- جعفری لنگرودی ، محمد جعفر ، ترمینولوژی حقوق ، کتابخانه گنج دانش، ۱۳۸۸
- ترکی ، غلامعباس ، نگرش علمی و کاربردی ، قانون جرایم رایانه ای ، ماهنامه دادرسی، شماره ۸۳ ، ۱۳۸۹
- علی نژادی ، محسن و علی نژاد ، زهرا ، مقاله اعتبار داده پیام در قرار دادهای داخلی و بین المللی در تجارت الکترونیک، فصلنامه علمی، دوره سوم ، پاییز ۱۳۹۷
- حسن بیگی ، ابراهیم ، حقوق و امنیت در فضای سایبر، موسسه مطالعات و تحقیقات بین المللی ابرار معاصر ، تهران ۱۳۸۴
- بابایی ، جواد ، جرایم رایانه ای و آیین دادرسی حاکم بر آن، چاپ دوم، تهران مرکز مطبوعات و انتشارات قوه قضائیه ۱۳۹۷
- میر محمد صادقی ، حسین، حقوق کیفری اختصاصی (۲) جرائم علیه اموال و مالکیت ، چاپ پنجاهم ، تهران ، میزان، ۱۳۹۶
- زراعت ، عباس ، حقوق جزای اختصاصی (۲) جرایم علیه اموال و مالکیت، تهران، جاودانه، جنگل، ۱۳۹۲
- خرم آبادی ، عبدالصمد، کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیت ایران فصلنامه مطالعات حقوق خصوصی دانشگاه تهران ، سال سی و هفتم ، شماره ۲ تابستان ۱۳۸۶

9th International & National Conference on
Management Studies, Accounting & Law
December 20th & 21th, 2023 | University of Tehran

Archive of SID



نهمین کنفرانس بین المللی و ملی مطالعات مدیریت، حسابداری و حقوق
۲۹ و ۳۰ آذر ۱۴۰۲ | دانشگاه تهران

سالاری، مهدی، حقوق کیفری اختصاصی، کلاهبرداری و ارکان متشکله آن، چاپ دوم، تهران، میزان، ۱۳۹۳
نظریه مشورتی اداره حقوقی قوه قضائیه به شماره ۷/۹۳/۱۱۶۱ مورخ ۱۳۹۳/۵/۱۸