همایش علمی مطالعات حقوقی، علوم قضایی و پژوهش های اجتماعی

نهاد برگزار کننده همایش: موسسه قانون یار

((باهمکاری و حمایت معنوی دانشگاه رهنورد (استان بلخ، کشور افغانستان) – جهاد دانشگاهی استان تهران))

سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی شماره مجوز: ۷۸۸۶۴-۱۵۲۱/۳۳۰۱

تاریخ برگزاری همایش: ۱۳خرداد۱۴۰۰ شماره مقاله: ۹۵/۱۷۹ رده بندی کنگره: الف ۹۰۳/۷۸۵۵

تحلیل کلاهبرداری رایانه ای و طرق پیشگیری از آن

مجید مولوی[۱]

کارشناس ارشد حقوق جزا و جرم شناسی

محمد باقر تاجی

کارشناس ارشد حقوق جزا و جرم شناسی

چکیده

در زندگی باهمادی (اجتماعی) امروز بشر تحول‌هایی صورت گرفته و با تأثیر از آن جرایم نیز اشکال متفاوتی به خود گرفته است که جرایم رایانه‌ای مصداق بارز این تحول‌ها درزندگی باهمادی (اجتماعی) انسان‌ها می‌باشد. با توجه به تحولات عظیمی که در عرصه تکنولوژی بوقوع پیوسته و انقلاب‌های مختلفی که در زمینه فن‌آوری اطلاعات و ارتباطات در طی چند سال اخیر شاهد ان بوده‌ایم و با توجه به کارکرد مثبت این فن‌آوری اما گاه دیده می‌شود که بعضی از افراد سودجو و فرصت طلب با فراگرفتن داشتن و مهارت لازم در پی سوء استفاده از کاربران و هم‌چنین ایجاد و بروز یک سری مشکلات هستند و خسارات فراوانی را به بار می‌آورند. لذا در بیشتر کشورهای دنیا جرایم اینترنتی بعنوان یک معضل حاد و بسیار مهم تلقی می‌گردد و لذا دولتها درصدد و به دنبال پیدا نمودن راه حل‌های مختلفی در جهت ریشه‌کن کردن و یا کم کردن یا حتی جلوگیری از جرایم مزبور می‌گردند.

واژگان کلیدی: *کلاهبرداری رایانه‌ای، پیشگیری وضعی، پیشگیری اجتماعی، پلیس فتا، مهندسی اجتماعی، کلاهبرداری اینترنتی، فیشینگ*

---

[۱] نویسنده مسئول

مقدمه

کلاهبرداری رایانه‌ای یکی از بزه‌های بسیار شایع و زیان‌بار فضای سایبراست و شاید اغراق و گزاف نباشد که بگویم کلاهبرداری رایانه‌ای یک بزه رایانه‌ای واقعی و مطلق نیست بلکه تنها به جهت فراگیری و خطرناک بودن در قانون جرایم رایانه‌ای پیش‌بینی شده است (عالی‌پور، ۱۳۹۰، ص ۲۷۲). کلاهبرداری رایانه عبارت است هرگونه تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود. یادگیری از طریق اعمالی نظیر وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه به‌طور غیرمجاز می‌باشد. از انجا که اولین و نخستین پرونده جرایم رایانه‌ای مربوط به قضیه الدن رویس که حسابدار یک شرکت آمریکایی در سال ۱۹۶۳ بود و در واقع به نوعی یک کلاهبرداری از طریق گنجاندن دستور العمل اضافی بود. (خداقلی ، ۱۳۸۳، ص ۲۲) لذا باید گفت که کلاهبرداری رایانه‌ای نیاز به بررسی جدی و ریشه ای دارد و از آنجا که باید گفت همیشه پیشگیری بهتر از درمان است و علاج واقعه قبل از وقوع باید کرد لذا به دنبال یک سری راهکار برای مقابله و پیشگیری از کلاهبرداری رایانه‌ای هستیم. در این گفتار به بررسی پیشگیری وضعی که به مطالعه محیط و شرایط پیرامونی آن و شامل مجموعه اقداماتی به منظور تسلط بر محیط است. در واقع پیشگیری وضعی تمرکز جرم‌شناسی بر شخص بزه دیده یا سبیل‌های جرم است. (نجفی ابرندآبادی، ۸۳، ص۸۳)پیشگیری اجتماعی که به تعبیر استاد گسن یکی از سه شاخه جرم شناسی کاربردی است نوع دوم منقسم شده‌ای است که بعد پیشگیری وضعی و در واقع فرد مجرم محور اقدامات است و حمایت از سبیل مطرح نیست (نجفی ابرندآبادی، ۱۳۸۳، ص ۸۳) پیشگیری اجتماعی شامل آن قسم از تدبیرات که در فرآیند رشد مداخله می کند و عوامل بزه را حذف و خنثی می کند. پلیس فتا به عنوان یکی از مهم‌ترین ارکان عدالت کیفری که به نوعی ضابط جرایم رایانه‌ای پیش‌بینی شده است به بررسی و کشف جرایم مذکور می‌پردازد و بعضاً هشدارهایی را به مردم می‌دهد که به نمونه‌های از آن اشاره خواهیم کرد. یکی از طرق ارتکاب کلاهبرداری رایانه‌ای مهندسی اجتماعی است که در ادامه به طور تفصیلی بیان می گردد و تفاوت اصلی در بحث این است که کلاهبرداری رایانه‌ای یا به تعبیری کامپیوتری اعم از اینترنتی است و دایره شمول بیشتری را در برمی گیرد.

بخش اول: تاریخچه کلاهبرداری رایانه‌ای

اولین کلاهبرداری رایانه‌ای را می توان به قضیه الدن رویس در دهه ۱۹۶۰ که در واقع تاریخ قطعی اولین سوء استفاده مالی است، دانست. رویس یک حسابدار شرکت در آمریکا بود که به علت اختلافش با شرکت، با گنجاندن دستورالعمل اضافی در برنامه‌های سیستم های رایانه‌ای شرکت، در قیمت کالاها تغییراتی را ایجاد نمود و مبالغ به دست آمده را به حساب خاصی واریز می کرد. او توانست در مدت شش سال بیش از یک میلیون دلار برداشت کند اما چون نتوانست سیستم را متوقف کند در نهایت خود را به مراجع قضایی معرفی و به ده سال حبس محکوم شد. (دزیانی، ۱۳۸۳ : ص ۳۹). نخستین و اولین پرونده مطروحه در زمینه جرایم رایانه‌ای در ایران در دهه ۱۳۷۰ و باید گفت شکایت شرکت نرم‌افزاری سینامند شرکت واژه‌پرداز مبنی بر تکثیر و فروش غیرمجاز نرم‌افزارهای تهیه شده شرکت نرم‌افزاری سینا که موجب صدور رای در تاریخ ۱۳۷۲ /۴/۳ در مورد نرم‌افزارهای کامپیوتری با استناد به قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ شد (پاکزاد، ۱۳۷۵ ، ص ۳۱) با توجه به مطالب مارالذکر و گفته شده و طبق سند نهایی جرایم رایانه‌ای در ایران یعنی قانون جرایم رایانه‌ای که مصوب پنجم خرداد ۱۳۸۸ است که مربوط به جرم‌انگاری رفتارهای قابل ارتکاب در فضای سایبرات در فصل سوم تحت عنوان سرقت و کلاهبرداری مرتبط با رایانه، به جرم انگاری کلاهبرداری رایانه‌ای مبادرت نموده است.

بخش دوم: کلاهبرداری رایانه‌ی و ارکان و عناصر آن

کلاهبرداری رایانه‌ای: از سوی کمیته تخصصی شورای اروپا در زمینه جرایم کامپیوتری در خصوص کلاهبرداری رایانه‌ای تعریفی بدین شرح ارائه شده است:

وارد کردن، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری یادگیر مداخلات در پردازش داده‌ها که بر نتیجه پردازش‌ها داده‌ها که بر نتیجه پردازش اثر بگذارد و موجب ضررهای اقتصادی یا هر تصرفی در اموال شخصی دیگر به قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یادگیری شود» (باستانی، ۱۳۹۰، ص ۵۰)

تعریف دیگر که در بیشتر سیستم‌های قانونی نسبت به کلاهبرداری است مانند، اتریش، دانمارک، فنلاندف آلمان غربی، یونان، ایتالیا، لوگزامبورگ، نروژ، سوئیس و سوئد است متضمن این امر است که شخصی فریب بخورد. (نوری، ۱۳۹۰، ص ۷۹-۷۸) از انجا که در این موارد « فریب» کامپیوتر کفایت نمی‌کند، قابلیت اعمال مقررات مربوط به کلاهبرداری در این کشورها، همیشه به این بستگی دارد که آیا مجرم شخصی را که مسئول کنترل داده‌ها بوده فریب داده است یا نه ؟ (نوری، ۱۳۹۰، ص ۷۹) با این حال، در بعضی کشورها مقررات مربوط به کلاهبرداری، به صورت موسع‌تری مورد تفسیر قرار می‌گیرد؛ برای مثال این موضوع با دقت در اصطلاح « مانور متقلبانه» در تعریف قانونی از کلاهبرداری (escroquerie) در بلژیک و فرانسه به خوبی روشن می‌شود. کلاهبرداری اینترنتی: در واقع یکی از جرایم یقه سفیدهاست که ساترلند که بنیان‌گذار این اصطلاح است در دو کتاب خود یعنی سارق حرفه‌ای ۱۹۳۷ و اصول جرم‌شناسی ۱۹۲۴ به بررسی بزهکاری یقه سفیدها می‌پردازد و آن را مطرح کند. (White collar criminality) و قلمرو مطالعات جرم‌شناسی را گسترده‌تر می‌کند(نجفی ابرندآبادی، ۱۳۹۰، ص ۵۵). کلاهبرداری اینترنتی عبارت است از: هرگونه کلاهبرداری که بوسیله برنامه‌های کامپیوتری و رایانه‌ای یا ارتباطات شبکه اینترنتی صورت گیرد مثلاً از طریق سایت‌ها (web) پست الکترونیک (email) یا اتاق‌های گفت و گو (chatrooms) در واقع کلاهبرداری اینترنتی به هر نوع طرح متقلبانه‌ای گفته می‌شود که یک یا چند بخش از اینترنت را به کار می‌گیرد تا درخواست‌های متقلبانه‌ای را به منظور بردن اموال و انجام معاملات جعلی با قربانیان احتمالی مطرح می‌سازد. تفاوت کلاهبرداری رایانه‌ای با اینترنتی در این است که در واقع کلاهبرداری کامپیوتری یا رایانه‌ای مفهوم اعم‌تر و عام‌تر نسبت به کلاهبرداری اینترنتی دارد و لذا دو مقوله جدا از هم هستند. در مقابل گفته شده است کلاهبرداری رایانه‌ای یا کامپیوتری قبل از به وجود آمدن اینترنت بوده است ولی بعد از آنکه اینترنت به وجود آمد و محیط مجازی (cyberspace) کم کم و به مرور زمان اصطلاح کلاهبرداری کامپیوتری به کلاهبرداری اینترنتی تغییر نام پیدا کرد و عده‌ای معتقدند که کلاهبرداری رایانه‌ای همان کلاهبرداری اینترنتی می‌باشد و این دو اصطلاح را به جای هم به کار می‌برند .

بخش سوم: ارکان کلاهبرداری رایانه‌ای

۱- رکن قانونی : منظور از عنصر قانونی جرم اصل قانونی بودن جرم است. این اصل در متم قانون اساسی و قانون مجازات عمومی ایران پذیرفته شده است. (باهری، ۱۳۸۴، ص۱۰۹) در حال حاضر در اصل ماده دوم بیست و دوم قانون اساسی هم به این مسئله اشاره شده است. اصلی‌ترین سند عنصر قانونی بودن جرم ماده دوم قانون مجازات اسلامی ایران است که مقرر می‌دارد « هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد جرم محسوب می‌شود» اصل قانونی بودن جرم در قرن هیجدهم پدید آمد و بکار یا صراحتاً در کتاب خود به نام « جرایم و مجازات‌ها» که به سال ۱۷۶۴ منتشر شد از آن دفاع نمود . (باهری، ۱۳۸۴، ص ۱۱۱) مجموعاً در ارتباط با کلاهبرداری رایانه‌ای از جانب کشورهای جهان سه رویکرد در امر قانون‌گذاری اتخاذ شده است .

الف) برخی از کشورها صراحتا مقررات جزایی جداگانه‌ای در ارتباط با کلاهبرداری رایانه‌ای وضع کرده‌اند که عملا در این کشورها دو نوع کلاهبردرای وجود دارد: کلاهبرداری سنتی و کلاهبرداری رایانه‌ای، مثل مواد ۹۳ و ۱۱۵ قانون جرایم اقتصادی مرتبط با رایانه مصوب ۱۹۸۵ یا ماده ۳۶۳ قانون جزای آلمان اصلاحی ۱۹۸۶ و یا ماده ۲۷۹ قانون جزای دانمارک مصوب ۱۹۸۵ که در این کشورها تحصیل مال یا منفعت از طریق روش‌های غیرقانونی داده‌پردازی یا محو یا تغییر یا ایجاد داده در سیستم رایانه‌ای به عنوان کلاهبردرای رایانه‌ای شناخته شده است. (عالی‌پور، ۱۳۹۰، ص ۲۷۸)

ب) برخی از کشورها هر چند مقرره جدیدی برای کلاهبردرای رایانه‌ای وضع نکرده‌اند اما با وضع یک مقرره کلی بیان کرده‌اند که چنانچه جرمی از طریق رایانه ارتکاب یابد براساس مقررات کیفری فعلی (سنتی) قابل مجازات است مثل قانون جزای هند. در حقوق جزای ایران هم نسبت به جرایمی که نظامیان از طریق سیستم رایانه‌ای مرتکب می‌شند، همین سایت اتخاذ شده است. (عالی‌پور، ۱۳۹۰، ص ۲۷۸)

ج) برخی کشورها نیز اصولاً نسبت به جرم کلاهبرداری رایانه‌ای سکوت اختیار کرده‌اند و جرایم مرتبط با آن را با مقررات کیفری موجود پاسخ می‌دهند. این دسته از کشورهای عمدتاً در حال

توسعه هستند که رایانه و اینترنت هنوز به‌طور کامل در آنها رشد نیافته است. (عالی‌پور، ۱۳۹۰، ص ۲۷۸)

با توجه به مطالب فوق‌الذکر ایران در خصوص کلاهبرداری رایانه‌ای جز دست اول به شمار می‌آید که در واقع در مورد کلاهبرداری سنتی طبق قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری که در ماده یک به جرم مذکور اشاره می‌کند و در مورد کلاهبرداری رایانه‌ای هم قانون‌گذار طبق ماده ۱۳ قانون جرایم رایانه‌ای (۷۴۱ قانون مجازات اسلامی) کلاهبرداری رایانه‌ای را به این شکل معرفی می‌کند: هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰) ریال یا یکصد میلیون (۱۰۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

رکن مادی : شرط تحقق جرم آن است که قصد سوء با ارتکاب عمل خاصی دست کم به مرحله فعلیت برسد. فعل یا عمل خارجی که تجلی نیت مجرمانه و یا تقصیر جزایی است عنصر مادی جرم را تشکیل می‌دهد (اردبیلی، ۱۳۸۰، ص ۲۰۸).

عنصر مادی جرم در واقع حقیقت و ماهیت عمل ضد اجتماعی است و آن رفتار آدمی بر طبق نشانه‌هایی است که قانون‌گذار در متن قانون از آن به دست داده است یعنی رفتار آدمی غیر از پندار او است، در حقوق جزا پندار انسان هر چند زشت و نکوهیده باشد قابل مجازات نیست (باهری، ۱۳۸۴ ، ص ۱۹۲). عنصر مادی و ضروری جرم گاه رفتاری[1] است که در وضع خاصی از انسان بروز می‌کند و گاه به ندرت حالتی[2] است که بر او مستولی می‌گردد. (اردبیلی، ۱۳۸۰، ص ۲۰۹)

۱- Comporte ment

۲- Attitude

براساس ماده ۱۳ قانون جرایم رایانه‌ای (م ۷۴۱ قانون مجازات اسلامی) رفتار مادی فیزیکی جرم کلاهبرداری رایانه‌ای فعل است و آن هم از نوع مثبت زیرا مصادیقی که برای ارتکاب این جرم به کار برده شده است، نظیر وارد کردن، تغییر، محو و ... نوعاً به شکل مثبت است لذا کلاهبرداری رایانه‌ای با ترک فعل محقق نمی‌شود. (الهی‌منش، سدره نشین ، ۱۳۹۱ ص ۸۵) عنصر دوم که در رفتار نمود پیدا می‌کند تحصیل است که دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خود و لازم نیست حتماً مال در دستان مرتکب جای بگیرد به عنوان مثال کسی به سامانه بانک رخنه کند و رقم پولی دارنده حسابی را کاهش و یا حساب خود را افزایش دهد (عالی‌پور، ۱۳۹۰ ، ص ۲۸۱). تحصیل مال یا منفعت و مانند آن برخلاف کلاهبرداری سنتی به معنای دارا شدن نیست بلکه ممکن است کسی با وارد شدن به سامانه یک موسسه مالی، درصد اقساط وامی را که باید برگرداند کاهش دهد یا با دستکاری در سامانه، چنان بنماید گوید برخی از اقساط وام پرداخت شده است مرتکب کلاهبرداری رایانه‌ای شده است (عالی‌پور،۱۳۹۰،ص ۲۸۱)

رکن روانی: عنصر روانی که برای مسئولیت مورد توجه است در دو مطلب باید مورد توجه قرار گیرد.

۱- اراده انجام جرم آن‌چنان که مقنن یا قانونی مشخص کرده است. ۲- آگاهی جرم بر این مطلب که دارد از ممنوعیت‌های قانون تجاوز می‌کند این نکته مبنای سوء نیت عام است مثلاً قانون می‌گوید هرکس عامداً این کار را انجام دهد گاهی هم ممکن است نگوید. (نوربها، ۸۹ ص ۱۵).

برای تحقق جرم نقض اوامر و نواهی قانون‌گذار به تنهایی کافی نیست. فعل مجرمانه باید نتیجه خواست و اراده فاعل باشد، به سخن دیگر، میان فعل مادی و حالات روانی فاعل باید نسبتی موجود باشد تا بتوان مرتکب را مقصر شناخت. (اردبیلی، ۱۳۸۰، ص ۲۳۳). جرم کلاهبرداری رایانه‌ای در زمره جرایم عمدی است که متضمن وجود سوءنیت عام و خاص است. سوء نیت عام عبارت از عمد ارتکابی اعمالی از قبیل، وارد کردن، تغییر، محو و ... است؛ یعنی فرد مرتکب جرم « شخص یا اشخاص حقیقی یا حقوقی) ، «عالماً» «عاملاً» افعال مذکور را انجام دهد . (الهی

منش، سدره‌نشین، ۱۳۹۱، ص ۸۶). در کلاهبرداری رایانه‌ای در واقع باید گفت که قصد نهایی بایسته نیست و وجود آن ضروری نیست. (عالی‌پور، ۱۳۹۰، ص ۲۸۴).

بخش چهارم: طرق و شیوه‌های ارتکاب کلاهبرداری رایانه‌ای

۱- مهندسی اجتماعی: (Social Engineering)

حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون درخصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه (قلی زاده نوری، ۱۳۸۱، ص ۶۸۸) مهندسی اجتماعی نوعی نفوذ غیرمجاز یا هک شفاهی به شمار می‌رود که در آن مرتکب با تماس تلفنی یا ارتباط از طریق پست الکترونیک یا گپ‌زنی یا معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبر سعی در تخلیه اطلاعاتی مخاطب خود پیرامون سیستم رایانه‌ای مربوطه می کند. در واقع آنچه به چشم می‌آید. این است که در مهندس اجتماعی، مرتکب قبل از این‌که به دانش فنی مربوطه به نفوذ به سیستم رایانه‌ای متکی باشد، متکی به میزان نفوذ کلامی یا رفتاری او دارد که به شیوه ی خطر ناکی در حال افزایش است . مهندسی اجتماعی اگرچه مقدمه کلاهبرداری رایانه‌ای است ولی از مقدمات بعیده است و می تواند معادل توسل به وسایل متقلبانه در نظر گرفته شود البته شایان به ذکر است که چه بسا هدف مهندسی اجتماعی کسب و به دست آوردن اطلاعات مالی نباشد و ممکن است به دنبال اطلاعات امنیتی شرکت یا سیستم یا اصولاً نوعی اصلاح یا بی‌هدف باشد (عالی‌پور، ۱۳۹۰، ص ۲۷۳).

۲- فیشینگ یا کسب اطلاعات ملی: (Phishing)

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶ رقمی عابر بانک، رمز دوم cvv2 را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند. شبکه‌های حراجی و درگاه‌های پرداخت آنلاین نمونه‌ای از ابزارهای الکترونیکی ارتباطات می‌باشد. (پلیس فضای تولید و تبادل اطلاعات). کلاهبرداری فیشینگ از طریق ایمیل‌ها و پیام‌ها صورت می‌پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در یک وب سایت‌های جعلی

که در ظاهر کاملاً شبیه وب سایت‌های سالم و قانونی می‌باشد وارد می‌نماید. (پلیس فضای تولید و تبادل اطلاعات).

۳- حمله نفوذگر (Pharming)

حمله نفوذگر[1] به منظور تغییر ترافیک وب سایت به یک وب سایت جعلی دیگر است. در این بخش از شیادی، با دستگاری سرویس دهنده DNS توسط فرد شیاد که در اصطلاح فنی به « سمی[2]» شدن سرویس دهنده DNS کاربر معروف است. منجر می‌شود. کاربر به تصور این‌که وارد سایت اصلی بانک می‌شود وارد سایت جعلی فرد شیاد شده و اطلاعات محرمانه بانکی اعم از شماره حساب، شماره کارت و کلمه عبور را وارد می‌کند و آن‌گاه فرد شیاد به راحتی می‌تواند نسبت به سوء استفاده اقدام کند. (سبحانی، جوکار، ۱۳۹۱،)

۴- فرآیند کپی کردن (Skimming) :

فرآیند کپی کردن اطلاعات نوار مغناطیسی کارت اعتبار مشتری از طریق کشیدن کارت از میان کارت‌خوان و استفاده از اطلاعات جهت ساخت کارت تقلبی توسط فرد شیاد را (Skimming) می‌نامند. (سبحانی، جوکار ،۱۳۹۱).

۵- دزدیدن کلمه عبور (Shoulder surfing)

دزدیدن کلمه عبور دارنده کارت هنگام استفاده از دستگاه خودپرداز یا پایانه فروش از طریق مشاهده کاراکترهای وارد شده توسط کاربر را شامل می‌شود. (سبحانی، جوکار،۱۳۹۱) مفهوم پیشگیری از جرم: برخی پیشگیری از جرم را نوعی مداخله از طریق اتخاذ تدابیر برای جلوگیری یا کاهش خطرات ارتکاب یا کاهش نتایج احتمالی می‌داند (ابراهیمی، ۱۳۹۱، ص ۳۸).موریس کوسن جرم‌شناس کانادایی پیشگیری را چنین تعریف می‌کند « مجموعه اقدامات و تدابیر قهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم، کاهش وخامت جرم، پیرامون

۱- Hacker

۲- Poisoned

علل جرایم اتخاذ می‌شود (ابراهیمی، ۱۳۹۱، ص ۳۸). مفهوم پیشگیری بر پایه این نکته بنا می‌شود که در پیرامون جرم و بزه‌دیدگی عوامل بسیار زیادی دخیل هستند. دامنه این عوامل بسیار وسیع است؛ شرایطی که افراد در آن رشد می‌کنند. شرایط بومی و محلی، موقعیت‌ها و فرصت‌های تسهیل کننده جرم همگی در ایجاد جرم و بزه‌دیدگی دخیل هستند (جوان جعفری، سید زاده ثانی، ۱۳۹۱،ص ۳۸) جرم‌شناسی پیشگیرانه (Preventional criminology) که به تعبیر استاد گسن یکی از سه شاخه جرم‌شناسی کاربردی است در یک تقسیم‌بندی کلی منقسم می‌شود به پیشگیری وضعی و پیشگیری اجتماعی (نجفی ابرندآبادی، ۱۳۸۳، ص ۸۳) پیشگیری وضعی از کلاهبرداری رایانه‌ای: پیشگیری وضعی یعنی تغییر اوضاع و احوال و شرایط خاص- که احتمال ارتکاب جرم در آن زیاد است- به منظور دشوار نمودن، خطر پر کردن یا جاذبه‌زدایی ارتکاب جرم این نوع از پیشگیری از لحاظ مبانی و شویه ها کاملاً با دیگر گونه‌های پیشگیری متفاوت‌اند (ابراهیمی، ۱۳۹۱، ص ۸۶). پیشگیری وضعی عبارت است از تغییر در موقعیت‌های خاصی که ارتکاب جرم در آن زیاد است به منظور دشوار نمودن بر خطر کردن یا جاذبه‌زدایی برای کسانی که قصد ارتکاب دارند (ابراهیمی، ۱۳۹۱، ص ۸۹)در واقع پیشگیری وضعی با تمرکز بسیار زیاد بر فرصت‌های مجرمانه، سخت کردن سبیل‌های جرم و افزایش نظارت است که پیش می‌رود. (جوان جعفری، سیدزاده ثانی، ۱۳۹۱، ص ۵۱).در زمینه پیشگیری وضعی از جرایم رایانه‌ای باید گفت که با این‌که مشکلات زیادی بر سر راه آن وجود دارد اما باز هم جایگاه خاصی برخوردار است. یکی از این دلایل توجیه می‌تواند قابلیتی باشد که فضای سایبر فراهم آورده است. (فراهانی، ۱۳۸۳، ص ۱۰۸)از جمله اقدامات خاص پیشگیری وضعی از جرایم رایانه‌ای می‌توان به موارد ذیل اشاره کرد:

۱- نصب دیواره آشین[۱]یا لایه[۲]در شبکه‌های اطلاع رسانه رایانه‌ای (فراهانی،۱۳۸۳،ص۱۰۹)

۱- Fire wall

۲- filltering

۳- Cyber patrl

۲- پلیس گشت سایبر[۱] یکی از نتایج مثبت پلیس گشت پیاده به عنوان یک اقدام وضعی پیشگیرانه است (فراهانی، ۱۳۸۳، ص ۱۰۹).

۳- برنامه‌های ویروس‌یابی یا کوکی‌یابی (فراهانی، ۱۳۸۳، ص ۱۰۹).

۴- استخدام یک کارمند امنیت رایانه و نیز مشاوران رایانه‌ای (رحمانی، ۱۳۹۰)

۵- یک خط تلفن اضطراری برای گزارش کلاهبرداری رایانه‌ای و یا تقلب (رحمانی،۱۳۹۰).

۶- استفاده از هکرها برای کمک به شناساندن ضعف سیستم‌های امنیتی موجود.

(پلیس فضای تولید و تبادل اطلاعات).

۷- استفاده ا ز پلیس و سازمان‌های خود نظارتی مثل بانک و بیمه خود یک راه پیشگیرانه است. (ص ۱۰ ، ۱۹، Levi)

۸- تقویت سیستم امنیتی حفاظتی بانک و سیستم‌های و شرکت‌های مالی (یلی، ریس پلیس فتای خراسان شمالی ۱۳۹۱)

۹ - تشکیل ستاد پیشگیری و مبارزه با جرایم فناوری اطلاعات در محیط سایبر

(قریشی، ۱۳۹۱).

۱۰- مجهز کردن بانک و کلیه موسسات ملی به سیستم‌های حفاظتی و امنیتی برای رایانه‌ها

۱۱- حفاظت فیزیکی[۲]: حفاظت فیزیکی به معنای حفظ رایانه، تجهیزات رایانه، رسانه‌های رایانه‌ای و تمامی سیستم، در مقابل سوانح طبعی، نواع مختلف حوادث و محلات عمومی است. (میرمحمدصادقی، شایگان، ۱۳۸۶، ص ۱۱۹).جرایم رایانه‌ای قابل پیش‌بینی نیستند پس در واقع نیاز به تدابیری برای دشوار کردن ارتکاب آنها نمود اولین حلقه حفاظت فیزیکی اقداماتی است که مجرمین را از نفوذ به ساختمان محل استقرار رایانه‌ها مأیوس نمود به‌طوری که تدابیر مناسب

۱- Physical security'

برای ورودی ا تاق‌های محل نگهداری سیستم رایانه‌ای اتخاذ شودو هم‌چنین جهت جلوگیری از استراق سمع تلفنی، اتخاذ تدابیر و اقدامات لازم جهت حفاظت از رمز عبور، نام فایل ها و سایر اطلاعات محرمانه ضروری است. (میرمحمد صادقی، شایگان، ۱۳۸۶، ص ۱۱۹).

۱۲- حفاظت کارکنان[۱]: تدبیر حفاظت کارکنان، افرادی را پوشش می‌دهد که به نحوی مجاز به کار با سیستم می‌باشد اغلب جرایم مالی رایانه‌ای توسط افراد مذکور و نه حریم‌شکنان صورت می‌گیرد. در ضمن قابل ذکر است که در این‌باره و در بحث حفاظت کارکنان بایستی دیدیترین احتیاط‌ها در مورد کارکنان اخراجی یا کارکنانی که داوطلبانه از کار کناره‌گیری می‌کنند اتخاذ شود. (میرمحمدصادقی، شایگان، ۱۳۸۶، ص ۱۱۹).

۱۳- حفاظت از ارتباطات:[۲] گونه‌ای دیگر از تدابیر امنیتی و حفاظتی، حفاظت ارتباطات است که شامل حفاظت از پست، مخابره، تلفن، ارتباطات پست صوتی و هم‌چنین حفاظت از اطلاعات انتقال داده شده از یک رایانه به رایانه دیگر از طریق انتقال شبکه می‌شود. مجرمین حرفه‌ای ممکن است سیستم رایانه را برای ارتکاب کلاهبرداری یا مستقیماً برای منفعت خودشان مورد هدف قرار دهند. در این صورت تدابیر حفاظت ارتباطات، (به عنوان نمونه کلمات رمز عبور) مهم‌ترین عامل برای ذور نگهداشتن مجرمین حرفه‌ای است. (میرمحمد صادقی، شایگان، ۱۳۸۶، ص ۱۲۰).

۱۴- حفاظت عملیات:[۳] آخرین نوع از تدابیر حفاظتی، حفاظت عملیات است. حفاظت عملیات به معنی وضع تدابیری جهت شناسایی و مقابله با تهدیدهایی است که سیستم‌ها را به مخاطره می‌اندازد. (میرمحمد صادقی، شایگان، ۱۳۸۶، ص ۱۲۱).

۱۵- استفاده از کد رفتاری: کد رفتاری عبارت است از مجموعه قواعد و مقرراتی راجع به حقوق نرم‌افزار که مشتمل بر تظیم قواعد سازمان‌های تخصصی، کدهای رویه‌های هماهنگ، کدهای رفتاری، کدهای اخلاقی و شغلی می‌باشد که مجموعاً کدهای رفتاری نامیده می‌شود (باستانی،

۱- personnel sccurity

۲-communications security

۳-operations security

۱۳۹۰، ص ۱۲۹). پیشگیری اجتماعی: پیشگیری اجتماعی به فرآیند تربیت و رشد انسان تکیه می‌کند و راهبرد نسبتاً زمان‌بری برای پیشگیری از جرم ترسیم می‌کند. این نوع از پیشگیری در ایران علاوه بر صدر بند ۵ اصل ۱۵۶ قانون اساسی که « اصل راهبردی» حقوق پیشگیری ایران محسوب می‌شود، در اصول راهبردی دیگر قانون اساسی نیز مورد اشاره قرار گرفته است. (ابراهیمی، ۱۳۹۱، صص ۶۲ – ۶۱).

پیشگیری اجتماعی در واقع خود به دو دسته تقسیم می‌گردد که عبارت است:

۱- پیشگیری اجتماعی رشدمدار یا زودرس : در واقع مداخله در رشد و شخصیت فرد مثل کودک برای جلوگیری از جرم او در آینده دارد و در واقع هدف از پیشگیری اجتماعی رشدمدار آموزش و تربیت افراد برای پیشگیری از جرم در آینده است در واقع این‌گونه از پیشگیری را آموزش و پرورش محور هم می‌نامند. (ابراهیمی،۱۳۹۱،ص۶۱).

۲- پیشگیری اجتماعی جامعه‌مدار: هدف از تدابیر پیشگیری اجتماعی جامعه‌مدار، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به وسیله دو اقدام اصلی است ۱- ترغیب و تسهیل بروز انگیزش‌های مشروع و سودمند ۲- برحذر داشتن از ناهنجاری‌های سایبری (میرمحمد صادقی، شایگان، ۱۳۸۶، ص ۱۱۶).

بخش پنجم: پیشگیری اجتماعی از کلاهبرداری رایانه‌ای

الف) پیشگیری اجتماعی رشدمدار یا زودرس

۱- ارائه آموزش کافی و اطلاع‌رسانی به هنگام در مدارس و آموزشگاه‌های که کودکان در حال تحصیل هستند.

۲- آگاه و مطلع کردن کودکان از خطرات و معضلات فضای سایبر

۳- برگزاری کلاسهای آموزشی و همایش در مدارس

۴- آموزش والدین برای آشنایی کودکان از جرایم محیط سایبر

۵-هدایت گودکتن به سمت استفده درست

۶- استفاده از هوش بالا و زیاد کودکان در جهت درست

۷- آشنا کردن کودکان با اخلاقیات کامپیوتر و احساس مسئولیت در قبال رفتارشان (باستانی، ۱۳۹۰، ص ۱۳۱).

۸- همکاری مدارس با نهادهای متولی آموزش رایانه‌ای برای پیشگیری

ب) پیشگیری اجتماعی جامعه‌مدار

۱- دسترسی به فناوری‌های بازدارنده که این کار مستلزم محیط نظارتی متناسب است. (خبرگزاری دانشجویان ایران)

۲- آگاهی از خطرات بالقوه امنیتی و روش مقابله با آنها

۳- همکاری مناسب میان تمام عوامل دخیل و تأثیرگذار

۴- وجود موازین قانونی لازم ماهوی و مشکی با ملاحظه به حقوق کیفری بین‌المللی

۵- ارائه آموزش عمومی به شهروندان و بالابردن سطح معلومات (رضوی فرد، ۱۳۹۱).

۶- جدیت و تلاش در مبارزه و مقابله با جرایم یقه سفیدها (جلالی فراهانی، ۱۳۸۳، ص۱۰۴)

۷- افزایش تدابیر آموزشی بالا در تمام سطح جامعه برای گروهای حکایتی(میرمحمدصادقی، شایگان، ۱۳۸۶، ص ۱۱۶).

۸- ابزارهای کافی و مناسب در اختیار شهروندان قرار دادن

۹- تعامل بانک و شکرت‌های مالی با پلیس فضای تولید و تبادل اطلاعات

۱۰- فیلتر و پالایش شبکه‌های اجتماعی نظیر فیس بوک

بخش ششم: پیشگیری کیفری از کلاهبرداران رایانه‌ای

بهترین روش مقابله با ارتکاب جرم توسط مجرمین سایبری از نوع یقه سفید که عمدتاً از قوانین هم اگاهی دارند نشدید کیفر و در عین حال افزایش دخالت حقوق کیفری با توسعه مجازات‌هاست تا در موارد لازم با تشخیص قاضی کیفرهای مثل مجازات‌های اجتماعی با جایگزین زندان در نظر گرفته شود تا استعداد و خلاقیت مجرم سایبری در مدت محکومیت تباه نگردد. (عالی‌پور، ۱۳۹۰، ص ۲۹). وجود بزهکار نه فقط نظم اجتماعی را به خطر می‌اندازد بلکه قدرت دولت را نیز تضعیف و تهدید می‌کند و لذا دولت به شدت درصدد سرکوبی بزهکاری و به خصوص بزهکاران برمی‌آید. (میرمحمدصادقی، شایگان، ۱۳۸۶، ص ۱۲۱). در ضمن در سیاست جنایی نیز مسئله مقابله با جرم نهفته است و چگونگی و کیفیت و انتخاب نوع کیفر و برخورد با بزهکاران نیز بیان می‌شود. (میرمحمد صادقی، شایگان، ۱۳۸۶، ص ۱۲۱)

نتیجه‌گیری

یکی از جرایم مالی که در حوزه سایبر و فضای مجازی و رایانه اتفاق می‌افتد کلاهبرداری رایانه‌ای است در واقع باید گفت از آن‌جا که این جرم خسارت جبران‌ناپذیری را در بردارد و چه بسا موجب نگرانی افراد از دارایی و اموال خود می‌گردد از آن‌جا که کلاهبرداری به تعبیری مختص افراد باهوش و زیرک است و به نوعی افرادی که از خطاها و نقص‌های موجود اطلاع دارند لذا باید گفت در پی پیشرفت‌ها و تحولات اجتماعی است که این افراد فریب‌کاری‌های خود را در سایه افزارهای به وجود آمدهف پیچیده‌تر و ناشناخته‌تر می‌سازند و اگر احساس کند که راه‌های فریب و نیرنگ در معرض شناخته شدن قرار می‌گرد به دنبال فرصت‌های نو برای ارتکاب جرم خود می‌گردند. از آن‌جا که راه‌های کلاهبرداری رایانه‌ای را ذکر کردیم و دیدم که به راحتی می‌توان دست به کلاهبرداری رایانه‌ای زد لذا هیچ کس مصون از جرم مذکور نیست لذا باید درصدد آن برامد که از جرم مذکور پیشگیری گردد. از هر سو و نظر که کلاهبرداری رایانه‌ای به واسطه عدم شناخت کافی یا عدم مهارت لازم در سیستم‌های رایانه‌ای و یا نبود راهکاری مناسب برای مقابله با جرم مذکور است در مطالب فوق الذکر به راه‌های برای مقابله با کلاهبردرای رایانه‌ای اشاره شد. آنچه مهم است این است که جرایم رایانه‌ای و به طور خاص کلاهبرداری رایانه‌ای برای مقابله و پیشگیری با آن و یا عدم تکرار دوباره جرم نیاز به همکاری

و همیاری تمام رشته‌ها و حوزه‌های علوم نظیر علوم اجتماعی، روان‌شناسی، جامعه‌شناسی، فناوری اطلاعات و ... می‌باشد. باید گفت که فضای تبادل اطلاعات و حقوق فناوری اطلاعات چیزی نیست که به راحتی از آن بگذریم و عطایش را به لقایش ببخشیم بلکه چون هم ما نیاز به استفاده از فضای مجازی و سایبری داریم لذا باید چالش‌های موجود را سیاست‌گذاران در عرصه‌های خرد و کلان کشور با اتخاذ تدابیر مناسب که موجب رشد و شکوفایی افراد جامعه در تمامی ابعاد فراهم آورد. قابل ذکر است که در بحث امنیت و حفاظت از سیستم‌های رایانه‌ای، امنیت به معنی مطلق و تمام آن وجود ندارد و همواره دست‌یابی افراد به شیوه‌های نوین و جدید ارتکاب جرم کلاهبرداری رایانه‌ای در محیط سایبر انجام می‌گیرد و لذا این ما را بر آن می‌دارد که به دنبال یک مبارزه مؤثر و منسجم با این جرم با پایه شناخت درست از ماهیت و شیوه‌های ارتکاب آن است. در آخر باید گفت از آن‌جا که گاه پیشگیری کیفری جواب نمی‌دهد و مجازات هدف اصلی خود را یعنی اصلاح ندارد می‌توان دست به پیشگیری قبل از جرم زد و در این راستا در مورد کلاهبرداری رایانه‌ای می‌توان با آموزش و بالا بردن سطح اطلاعات والدین و دانش‌آموزان در پیشگیری اجتماعی زودرس و هم‌چنین کارگاه‌های آموزش عمومی در پیشگیری اجتماعی جامعه‌دار و هم‌چنین راهکارهای امنیتی و حفاظتی مناسب به منظور ریسک ارتکاب جرم دستگیری وضعی و مجموعاً با تقویت دانش مخاطبان سایبری و تقویت همکاری‌های بین‌المللی می‌توان به نوعی در برابر کلاهبرداری رایانه‌ای پیشگیری و مقابله کرد به امید روزی که شاید هیچ جرمی نباشیم.

منابع و مأخذ

۱-ابراهیمی، شهرام، جرم شناسی پیشگیری، جلد نخست، تهران ،میزان ، چاپ دوم ، ۱۳۹۱

۲-اردبیلی،مخمد علی، حقوق جزای عمومی، جلد نخست، تهران، میزان، چاپ دوم، ۱۳۸۰

۳-الهی منش- سدره نشین، محمد رضا- ابو الفضل، محشای قانون جرایم رایانه ای، تهران، مجد،چاپ اول، ۱۳۹۱

۴-باستانی، برومند، جرایم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری، تهران، بهنامی، چاپ سوم، ۱۳۹۰

۵- باهری، محمد، نگرشی بر حقوق جزای عمومی، تهران، مجد، چاپ دوم ، ۱۳۸۴

۶-پاکزاد، بتول، بزه های کامپیوتری،پیان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی،۱۳۷۵

۷-جلالی، امیر حسین، پیشگیری از جرایم رایا نه ای ،مجله حقوقی دادگستری، شماره ۵۴

۸- جوان جعفری – سید زاده ثانی، عبد الرضا – مهدی،رهنمود های عملی پیشگیری از جرم، تهران،میزان ، چاپ اول، ۱۳۹۱

۹-جوکار- سبحانی، پریا- مژگان، کارشناسان خدمان انفور ماتیک،۸فروردین ،۱۳۹۲

۱۰-خداقلی، زهرا، بزه های کامپیوتری،تهران، آریان،چاپ اول، ۱۳۸۳

۱۱-خرم آبادی، عبد الصمد،کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیت ایران،فصل نامه دانشکده علوم سیاسی،شماره ۲،۱۳۸۶

۱۲-آنجلیس، جینا، جرایم سایبر، ترجمه عبد الصمد خرم آبادی و سعید حافظی،تهران،دبیر خانه علی اطلاع رسانی، چاپ اول، ۱۳۸۳

۱۳-دزیانی ،محمد حسن، شروع جرم کامپیوتری/سایبری،خبرنامه انفورماتیک

۱۴-گفتگو با علی رحمانی،استاد دانشگاه الزهرا،۳۰آذر،۱۳۹۰

۱۵-گفتگوبا بهروز رضوی فرد، استاد دانشگاه علامه طباطبایی،۲۷آبان،۱۳۹۱

۱۶-عالی پور،حسن، حقوق کیفری فناوری اطلاعات، تهران، خرسندی،چاپ اول، ۱۳۹۰

۱۷- علی پور، حسن،جزوه درسی جزا اختصاصی(۱)دانشکده ادبیات و علوم انسانی دانشگاه شهرکرد،سال تحصیلی ۱۳۸۹-۱۳۸۸

۱۸-میر محمد صادقی- شایگان،حسین- محمد، راهکارهای مقابله با جرم کلاهبرداری رایانه ای در حقوق کیفری ایران،فصل نامه دیدگاه های حقوقی،دانشکده علوم قضایی و خمات اداری،شماره ۴۳-۴۲،۱۳۸۶

۱۹-نجفی ابرند آبادی، علی حسین، تقریرات جامه شناسی جنایی،دانشکده حقوق دانشگاه شهید بهشتی،سال تحصیلی ۱۳۸۴-۱۳۸۳،تنظیم مهدی صبوری پور

۲۰-نور بها، رضا،جزوه درسی عنصر معنوی جرایم،دانشکده حقوق دانشکده شهید بهشتی،سال تحصیلی ۱۳۹۰-۱۳۸۹

۲۱-اولریش، زیبر، جرایم رایانه ای، ترجمه محمد علی نوری،رضا نخجوانی،مصطفی بختیار وند،احمد رحیمی مقدم،تهران،گنج دانش،چاپ دوم، ۱۳۹۰

۲۲-گفتگو با سرهنگ یلی،ریس پلیس فتای خراسان شمالی ۲۰ بهمن، ۱۳۹۱

۲۳-LEVI،MICHACL،THE PREVENTION OF FRAUD، LONDONSW1H

۲۴-KUNZ-WILSON،M-P،COMPTERCRIME AND COMPUTER FRAUD,DEPARTMENT OF CRIMINOLOGY AND CRIMINAL JUSTICE,UNIVERSITY OF MARY LAND,2004

۲۵-WWW.FATA.IR

موسسه قانون یار

با همکاری مراکز علمی و دانشگاه های داخلی و خارج از کشور همچون
مرکز اطلاعات علمی جهاد دانشگاهی و نمایه مقالات در سایت sid.ir
(دانشگاه بین المللی رهنورد/بلخ/افغانستان)
(موسسه بین المللی ici world of journals/ورشو/لهستان)
(انجمن علمی بین المللی citefactor/فینیکس/آریزونا)
برگزار می کند:

همایش ملی
مطالعات حقوقی، علوم قضایی
پژوهش های اجتماعی

۱۳ خرداد ۱۴۰۰ - تهران

داوری زود هنگام مقالات

استان تهران-موسسه قانون یار

محورهای همایش:

* مقالات در گرایش های حقوق خصوصی، حقوق جزا حقوق عمومی، حقوق بین الملل، حقوق قضایی، فقهی و ....
* مقالات در گرایش های علوم ثبتی و علوم اقتصادی و بانکی
* مقالات در گرایش ها و موضوعات علوم اجتماعی و علوم تربیتی

روش های ارسال مقالات به همایش:

* ارسال فایل Word مقاله (به همراه شماره تماس) به ایمیل Phdsara@yahoo.com
* ارسال فایل Word مقاله به واتس آپ یا تگرام شماره ۰۹۱۰۰۶۳۶۰۰۲



به ده مقاله برتر و برگزیده همایش، ده تندیس به همراه تقدیرنامه مخصوص اعطا می گردد.
به مقالات ارسالی و پذیرفته شده پژوهشگران، گواهی نامه معتبر اعطا می گردد.
تمامی مقالات همایش در پایگاه ها و سایت های ملی و بین المللی نمایه و درج می گردند.
داوری مقالات حداکثر سه روز می باشد و گواهی نامه در کمتر از یک هفته صادر می شود.

جهت تقویت رزومه SID داوطلبان آزمون دکتری اساتید دانشگاه، قضات، وکلا

دبیرخانه: تهران، میدان انقلاب، خیابان اردیبهشت، پلاک ۱۹۲
واحد پذیرش مقالات:
۵۲۶ و ۶۶۹۷۹۵۱۹ - ۰۲۱
واحد صدور گواهی نامه:
۸۴ و ۴۴۴۴۱۷۶۴ - ۰۲۱
مشاور و راهنمای ارسال مقالات:
۰۹۱۹۶۷۴۸۶۲۵ ۰۹۱۰۰۶۳۶۰۰۲
www.Ghanonyar.ir www.Olomensani.ir