# بررسی بزه کلاهبرداری رایانه‌ای در قانون جرائم رایانه‌ای ایران و کنوانسیون جرائم سایبر

مهدی عبدی پور کشاورز[۱]- دکتر عباسقلی انصاری[۲]*- دکتر حمید ششگل[۳]

تاریخ دریافت: ۱۳۹۸/۱۰/۲۸- تاریخ پذیرش:۱۳۹۸/۱۲/۱

**چکیده:**

جرم کلاهبرداری به لحاظ گسترش دامنه و پیچیدگی آن در فضای مجازی (سایبر) موجب تحولات گسترده‌ای در زندگی بشر گردیده است. هرچند تدابیر کلی در مقابله با انواع روش‌های کلاهبرداری تقریبا مشابه است، اما با تفاوت‌های موجود در شیوه‌های گوناگون کلاه‌برداری بهره-گیری از روش‌های متناسب ضروروت میابد. بخشی از شیوه‌های مقابله نیازمند ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان در مورد مخاطرات سیستم‌های رایانه‌ای است و طبیعتا پس از آگاهی نظارت دائمی سازمان‌ها برروی سیستم رایانه‌ای و تدابیر امنیتی است.

هدف از تحقیق موردنظر، بررسی تاثیرات و تاثرات جرم کلاهبرداری در امنیت اجتماعی و قانون جرائم رایانه‌ای در جامعه می‌باشد. روش تحقیق حاضر به صورت توصیفی و تحلیلی بوده و در آن به تعریف، انواع و تفکیک کلاه برداری رایانه‌ای بانگاهی تحلیلی پرداخته شده است و النهایه راهکارهایی مناسب برای مقابله با آن ارائه گردیده است.

**واژگان کلیدی:** جرائم رایانه ای، امنیت اجتماعی، کلاهبرداری رایانه‌ای، انواع و تفکیک کلاهبرداری رایانه‌ای

---

[۱]- دانشجوی دکتری، حقوق کیفری و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، واحد کرج، دانشگاه آزاد اسلامی، البرز، ایران
Mahdi.abdipour1359@gmail.com

[۲]- استادیار و عضو هیئت علمی، گروه حقوق کیفری و جرم شناسی، دانشکده حقوق و علوم سیاسی، واحد تاکستان، دانشگاه آزاد اسلامی، قزوین، ایران: نویسنده مسئول
Bebaran@yahoo.com

[۳]- استادیار و عضو هیئت علمی،گروه حقوق عمومی، دانشکده حقوق و علوم سیاسی، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران
r.hamid_sheshgol@yahoo.com

**مقدمه**

پیدایش رایانه (سایبر) از بزرگترین تحولات فناوری در قرن ۲۰ ام به شمار می‌رود ولی هم-زمان با گستردگی این پدیده چالش‌های جدید نیز به چشم می‌خورد. نقض حریم زندگی خصوصی افراد و دستبرد به محتویات رایانه‌ها از جمله مشکلات جدید برای حقوق کیفری نوین جهت مبارزه با جرایم و مجرمان رایانه‌ای است. آنچه که مهم است این است که این پدیده به عنوان اثری تاثیرگذار در امنیت اجتماعی می‌باشد (جوکس[1] و یار[2]، ۲۰۱۳) تعیین دقیق اولین جرم رایانه‌ای دشواری است، برخی قضیه «آلدون رویس» آمریکایی در سال ۱۹۶۳ را اولین جرم رایانه‌ای می‌دانند که در این صورت می‌توان جرم کلاهبرداری را به عنوان اولین جرم سواستفاده مالی رایانه‌ای نام برد. الدون رویس حسابدار یک شرکت در آمریکا بود؛ وی به علت اختلافش با شرکت، با گنجاندن دستورالعمل‌های اضافی در برنامه‌های سیستم‌های رایانه‌ای شرکت، در قیمت کالاها تغییراتی را ایجاد کرده بود و مبالغ به دست آمده را به حساب‌های مخصوصی واریز می‌کرد. او توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما چون نتوانست عملکرد سیستم را متوقف کند در نهایت خود را به مراجع قضایی معرفی کرد و به ده سال حبس محکوم شد(دزیانی،۳۹:۱۳۸۳)، اما در ایران جرم رایانه‌ای سابقه چندانی ندارد لیکن گزارش‌های غیرپلیسی و غیرقضایی حکایت از تغییرات نمرات درسی، تغییر برخی اسامی پذیرفته شدگان کنکور در یال ۱۳۶۴ دارد. همچنین بیان شده که اولین جرم سایبری ناظر به عمل دانشجویان یزدی برای اسکن اسکناس و پرینت رنگی از آن در سال ۱۳۸۱ می-باشد. در مقاله حاضر، سعی گردیده جرم کلاهبرداری به عنوان رفتاری موثر در امنیت اجتماعی مورد نقد و بررسی قرار گیرد.

**تعریف جرم کلاهبرداری سنتی و رایانه‌ای**

حوزه جرایم در زندگی امروز بشر آن قدر پیچیده شده که قانون‌گذاران مجبورند تحولات جرم را به صورت مداوم زیر نظر داشته باشند و به تدوین قوانین صحیح گام بردارند، اما در زندگی اجتماعی بشر تحولاتی صورت گرفته که متعاقب آن، جرایم نیز اشکال متفاوتی گرفته-اند. جرایم اینترنتی و در صدر آن کلاهبرداری رایانه‌ای مصداق بارز این تحولات در زندگی اجتماعی انسان‌ها است. (نوری و دیگران، ۱۳۸۳) آنچه کلاهبرداری را از سایر جرایم علیه اموال

[1]- Jewekes
[2]- Yar

متمایز می‌کند، به کار بردن حیله و فریب است که همراه با پیشرفت‌های مادی و توسعه و تنوع روابط هر روز به نوعی جلوه می‌کند و شیوه‌های ارتکاب جرم کلاهبرداری رایانه‌ای را متنوع تر و به دام انداختن مجرمان را سخت‌تر کرده است. (باکر[1]، ۱۹۹۹)

کلاهبرداری به مفهوم ربودن عقل از شخص است و بدین اعتبار کلاه کسی را برداشتن به معنای فریب دادن و مال کسی را تصرف کردن یا به قصد عدم پرداخت، از دیگری قرض گرفتن است.

در متون فقهی از کلاهبرداری تحت عنوان احتیال و از کلاهبردار تحت عنوان محتال نام برده می‌شود. احتیال به معنای به کار بردن حیله است که مرتکب آن قصد وانمود کردن خلاف ظاهر را دارد و کشف حقیقت مستلزم تیزهوشی است. (شامبیانی،۱۳۸۲:۱۸۱) در زبان فرانسه Fraude به معنای حیله و تقلب و تدلیس است. در اصطلاح حقوقی، معنای کلاهبرداری از واژه Escroguerie است و Fraudel که با واژه انگلیسی Fraud و Deception مترادف است به معنای حیله و فریب آمده و از عناصر لازمه برای تحقق کلاهبرداری است. (اولریش، ۱۳۸۱)

ماده ۱ قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری که در حال حاضر عنصر قانونی جرم کلاهبرداری را در حقوق ایران تشکیل می‌دهد، اشعار می‌دارد: «هرکس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا کارخانه‌ها یا موسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیرواقع امیدوار نماید یا از حوادث و پیش‌آمدهای غیرواقع بترساند و یا اسم و یا عنوان مجعول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر، وجوه و یا اموال و یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها را تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و علاوه بر رد اصل مال به صاحبش به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود».

بدین ترتیب، ملاحظه می‌شود که قانون تعریفی از جرم کلاهبرداری ارائه نکرده است. به عبارت دیگر، در بیان جرم کلاهبرداری، قانونگذار به ذکر برخی از مصادیق آن پرداخته است. با توجه به همین مصادیق، می‌توان تعریف زیر را از جرم کلاهبرداری ارائه داد:

«کلاهبرداری عبارت است از بردن مال دیگری از طریق توسل توام با سوءنیت به وسایل یا عملیات متقلبانه». (میرمحمد صادقی،۱۳۹۴:۵۶) اوصاف جرم کلاهبرداری رایانه‌ای نیز همین

[1] -Baker

گونه است.

قانوگذار ماده ۱۳ قانون جرایم رایانه‌ای مصوب ۱۳۸۸را بدون تعریف، اختصاص به کلاهبرداری مرتبط با رایانه داده است. ماده مذکور مقرر داشته: «هر کس به طور غیر مجاز 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 ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد».

همانطور که ملاحظه می‌شود ماده مذکور کاملا متأثر از قوانین و مقررات بین‌المللی می-باشد. ولی در مقررات داخلی و بین‌المللی راجع به کلاهبرداری رایانه‌ای، این نکته مشترک وجود دارد که اولا شخص بدون مجوز اعمال متقلبانه روی داده‌ها انجام دهد یا سامانه را مختل کند. ثانیا وجه، مال یا مزایای مالی را تحصیل کند. بنابراین ملاحظه می‌شود که یکی از تفاوت-های اساسی بین کلاهبرداری رایانه‌ای و کلاهبرداری کلاسیک این است که تحقق کلاهبرداری کلاسیک مستلزم اغفال و فریب قربانی جرم است. در حالی که کلاهبرداری رایانه‌ای بدون فریب قربانی جرم، و از طریق مداخله ناروا در داده‌های رایانه‌ای یا عملکرد سیستم رایانه‌ای محقق می‌شود. (خرم آبادی،۹۲:۱۳۸۶) بدین ترتیب می‌توان کلاهبرداری رایانه‌ای را از نظر حقوقدانان اینگونه تعریف کرد: «تحصیل مال غیر با استفاده متقلبانه از رایانه». هرچند تعریف مذکور در زمان قانون تجارت الکترونیک ارائه شده اما می‌تواند با قانون جرایم رایانه‌ای منطبق باشد و به عبارتی بهترین و مختصرترین تعریف برای کلاهبرداری رایانه‌ای می‌باشد. در نتیجه می‌توان گفت در مواردی که رایانه به عنوان وسیله در کلاهبرداری استفاده می‌شود با تمام شرایط تعریف کلاهبرداری سنتی منطبق است ولی در مواردی که کلاهبرداری با استفاده متقلبانه از رایانه صورت می‌گیرد تعریف فوق شامل این موارد نمی‌شود.

کنوانسیون بوداپست تنها سند بین‌المللی که به مقررات ماهوی و شکلی جرایم رایانه‌ای می‌پردازد در ماده ۸ کلاهبرداری مرتبط با رایانه را اینگونه تعریف کرده است: «هرگونه اقدامات عمدی و غیر حق را که به قصد فریب یا دیگر مقاصد ناروا در راستای جلب منفعت اقتصادی غیر حق برای خود یا دیگری صورت می‌پذیرد. که این اقدامات غیر حق عبارتند از:

الف) هرگونه وارد کردن، تغییر، حذف یا متوقف سازی داده‌های رایانه‌ای

ب) هرگونه ایجاد اختلال در عملکرد یک سیستم رایانه‌ای».

نحوه نگارش ماده ۸ کنوانسیون به گونه‌ای است که سیستم رایانه‌ای را صرفا وسیله تحصیل منافع اقتصادی می‌داند و گویا از این موضوع غافل مانده است که اگر افعال فیزیکی «وارد کردن، تغییر داده، حذف یا متوقف سازی داده‌های رایانه‌ای»، منجر به تحصیل داده یا نرم‌افزارهای رایانه‌ای یا استفاده از عملکرد رایانه یا نرم‌افزارهای خاصی شود آیا باز هم کلاهبرداری شکل می‌گیرد یا خیر؟

البته شاید از «منافع اقتصادی» بتوان استفاده کرد و گفت که اگر داده دارای ارزش مالی بوده و منفعت اقتصادی داشته باشد، دو قسم از کلاهبرداری رایانه‌ای را پیش بینی کرده است. کلاهبرداری که رایانه در آن وسیله ارتکاب جرم است و کلاهبرداری که رایانه هم وسیله ارتکاب جرم و هم موضوع ارتکاب جرم است. (عالی پور، ۱۳۸۳: ۲۲۳-۲۲۴)

## انواع کلاهبرداری رایانه‌ای و تفکیک آن از عناوین مشابه

### انواع کلاهبرداری رایانه‌ای

مرکز دادخواهی کلاهبرداری اینترنتی امریکا پس از یک سال مطالعه و بررسی مستمر در سال ۲۰۰۱ در مجموع، کلاهبرداری رایانه‌ای را بر نه قسم دسته بندی کرد که در ذیل هر قسم انواع دیگری از مصادیق جرم قرار می‌گیرند:

الف) کلاهبرداری از مؤسسات مالی: در این قسم از کلاهبرداری رایانه‌ای، مرتکب از طریق سوء استفاده از کارت‌های اعتباری یا بدهی یا سرقت هویت دیگری و اتخاذ یک هویت جعلی مبادرت به فریب یک تجارتخانه یا سازمان می‌کند و سرمایه آن را تصاحب می‌نماید. این قسم از کلاهبرداری رایانه‌ای از حیث تعداد شکایت در راس سایر اقسام قرار دارد.

ب) کلاهبرداری در بازی: تقلب در شرطبندی از طریق تبانی ورزشی یا ادعاهای دروغین یا غیره برای بردن یک جایزه یا برنده شدن در مسابقه از دیگر اقسام کلاهبرداری رایانه‌ای است.

ج) کلاهبرداری در ارتباطات: در این قسم، کلاهبردار در فرایند مبادله اطلاعات و ارتباطات متوسل به تقلب می‌شود.

د) کلاهبرداری در کسب منفعت: در اینجا شخص حقیقی یا حقوقی با به کار بردن مانورهای متقلبانه، قوانین و مقررات موجود که برای استفاده از خدمات، وضع شده است را زیر پا گذاشته و به صورت غیرمجاز از آنها استفاده می‌کند. مثل نفوذ به سیستم رایانه‌ای اداره آب و برق و استفاده مجانی از آن.

ه) کلاهبرداری از بیمه: مرتکب در این قسم از کلاهبرداری در میزان خسارت واقعی وارد

شده بر خود، از طریق صحنه‌سازی یا ادعای دروغین تقلب می‌کند. حتی ممکن است مرتکب دچار هیچ‌گونه خسارتی نشده باشد اما با مانورهای متقلبانه خواستار جبران آن باشد.

و) کلاهبرداری از دولت: کلاهبرداری از دولت عبارت است از قلب عمدی حقیقت یا پنهان ساختن حقیقت یک موضوع به قصد انجام عملی به ضرر دولت، مشروط بر اینکه ضرر وارد شود. فرار از پرداخت مالیات یا وانمود کردن مبنی بر پرداخت مالیات یا تقلب در امور خیریه را می‌توان از ذیل این قسم از کلاهبرداری قرار داد.

ز) کلاهبرداری در سرمایه‌گذاری: عبارت است از به کار بردن اعمال خدعه‌آمیز در راستای سرمایه گذاری برای تحصیل پول یا سود بیشتر. طرح‌های پونزی و هرمی برجسته‌ترین قسم از اقسام سوء استفاده از سرمایه‌گذاری هستند.

ح) کلاهبرداری تجاری: این قسم از کلاهبرداری عبارت است از توسل به اینترنت برای قلب واقعیت از طریق اعمالی چون ورشکستگی به تقلب یا نقض حق مؤلف یا مترجم.

ط) کلاهبرداری از اعتماد دیگران: این نوع از کلاهبرداری با توسل به قلب حقیقت یا کتمان موضوع صورت می‌پذیرد که می‌تواند منجر به ضرر دیگری شود. حتی اگر قلب حقیقت موجب شود که دیگری شخصا به خود ضرری وارد سازد، در زمره همین قسم از کلاهبرداری است. تقلب در حراج اینترنتی یا عدم تحویل بهای کالای دریافت شده را می‌توان در شمار کلاهبرداری از اعتماد دیگران ذکر کرد. (سالاری،۱۳۸۶:۲۵۸)

اقسام گفته شده در کلاهبرداری همگی قابلیت ارتکاب در شبکه اینترنت را دارند، اما محدوده کلاهبرداری رایانه‌ای فراتر از این اقسام است و شامل مواردی که مرتکب یا قربانی جرم یا هر دو آنلاین یا داخل شبکه اینترنت نیستند، نیز می‌شود. مشهورترین کلاهبرداری رایانه‌ای که لزومی به ارتکاب از طریق شبکه اینترنت ندارد، کلاهبرداری از طریق کارت‌های به اصطلاح پلاستیکی می‌باشد که به سه گروه تقسیم می‌شوند:

گروه اول، کارت‌های دارای ارزش ذخیره شده هستند که ارزش مورد نظر به صورت الکترونیکی روی آنها ثبت شده و مشتریان برای انجام معاملات از آن استفاده می‌کنند.

گروه دوم، کارت‌های بدهی هستند که امکان می‌دهند عملیات و معاملات انجام شود و حساب های بانکی بلافاصله از طریق ارتباطات پیوسته ایجاد شده بین ماشین‌های تحویلدار خودکار و پایانه‌های انتقال وجوه الکترونیکی در محل فروش و بانک‌ها ثبت شود.

گروه سوم، کارت‌های اعتباری که برای خریداری کالا یا استفاده از خدمات، مورد استفاده

قرار می‌گیرند که پرداخت آنها موکول به زمان آینده می‌شود. (قناد، ۱۳۸۷)

**تفکیک کلاهبرداری رایانه‌ای از عناوین مشابه**

تنوع جرایم رایانه‌ای که اکثرا از طریق تغییر اطلاعات یا داده‌ها یا دستکاری رایانه صورت می‌گیرد، موجب شباهت جرایم رایانه‌ای مختلف از جهت عنصر مادی به یکدیگر است؛ و چون موضوع کلاهبرداری رایانه‌ای داده‌ها به عنوان نماینده اموال مادی در سیستم پردازش داده‌ها است (زبیر،۲۰:۱۳۸۱)، لذا با سایر جرایم رایانه‌ای ارتباط پیدا می‌کند. از آنجا که هدف مرتکب جرم کلاهبرداری رایانه‌ای سوء استفاده از رایانه با اختلال در سیستم رایانه‌ای برای جلب مال، منفعت، خدمات یا امتیازات مالی برای خود یا دیگری است این امر باعث تمایز بین کلاهبرداری رایانه‌ای با عناوین مشابه می‌شود. در ادامه به بررسی برخی از عناوین مشابه می-پردازیم. (شارلوت[1] و همکاران،۲۶۵:۲۰۰۱)

**الف) کلاهبرداری رایانه‌ای و سرقت رایانه‌ای:**

کلاهبرداری در مفهوم عام خود شامل سرقت رایانه‌ای نیز می‌شود. اما از آنجا که سرقت رایانه‌ای ناظر به سرقت داده‌ها و فایل‌ها است، علاوه بر اینکه یک جرم رایانه‌ای محض محسوب می‌شود، موضوع آن نیز صرفا مال نیست و از همین مجرا بین کلاهبرداری رایانه‌ای که منتج به تحصیل مال یا منافع مالی است و سرقت رایانه‌ای که منجر به ربودن داده‌ها و فایل‌های رایانه‌ای می‌شود، تفاوت حاصل می‌شود. در واقع رایانه در کلاهبرداری رایانه‌ای وسیله ارتکاب جرم است و در سرقت رایانه‌ای موضوع ارتکاب جرم.

**ب) کلاهبرداری رایانه‌ای و جاسوسی رایانه‌ای:**

جاسوسی رایانه‌ای دستیابی غیرمجاز به اطلاعات طبقه‌بندی شده سری و محرمانه و همچنین اسرار صنعتی و تجارتی است. جاسوسی رایانه‌ای صرفا یک جرم علیه امنیت تلقی نمی‌شود بلکه محدوده آن گسترده‌تر بوده و شامل دسترسی غیرمجاز به اسرار تجاری یا اطلاعات مالی یک شرکت نیز می‌شود؛ و از این مجرا می‌تواند مقدمه وقوع کلاهبرداری رایانه‌ای باشد، اما چون در جاسوسی رایانه‌ای مال یا منفعت مالی تحصیل نمی‌شود در زمره جرایم علیه اموال به شمار نمی‌رود. غالبا جاسوسی رایانه‌ای نسبت به جرم نفوذ غیرمجاز(هک) مؤخر و نسبت به کلاهبرداری رایانه‌ای مقدم است.

[1]- Charlotte

**ج) کلاهبرداری رایانه‌ای و حملات مهندسی اجتماعی:**

حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب‌پذیر شبکه؛ مهندسی اجتماعی نوعی نفوذ غیر مجاز یا هک شفاهی به شمار می‌رود که در آن مرتکب با تماس تلفنی و یا ارتباط از طریق پست الکترونیک یا گپ‌زنی و با معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبر، سعی در تخلیه اطلاعات مخاطب خود و پیرامون سیستم رایانه‌ای مربوط، می‌کند. در مهندسی اجتماعی، مرتکب پیش از اینکه به دانش فنی مربوط به نفوذ به سیستم رایانه‌ای متکی باشد، متکی به میزان نفوذ کلامی یا رفتاری خویش است.

مهندس اجتماعی هرچند مقدمه کلاهبرداری رایانه‌ای است ولی از مقدمات بعیده به شمار می‌رود و می‌توان آن را معادل توسل به وسایل متقلبانه در کلاهبرداری سنتی دانست. البته قابل ذکر است که طراح حمله مهندسی اجتماعی همواره به دنبال بدست آوردن اطلاعات مالی نیست و محتمل است که به دنبال اطلاعات امنیتی شرکت یا سیستم یا اصولا نوعی اطلاع‌یابی هدف باشد.

**د) کلاهبرداری رایانه‌ای و کسب اطلاعات مالی:**

کسب اطلاعات مالی نوعی مهندسی اجتماعی به شمار می‌رود. اما این مانع از آن نیست تا شخص از طریق نفوذ به سیستم رایانه‌ای «هک» اطلاعات مالی را کسب کند؛ که البته تفاوت کسب اطلاعات مالی با جاسوسی رایانه‌ای در این است که کسب اطلاعات مالی غالبا با نفوذ شفاهی به سیستم و جاسوسی رایانه‌ای با نفوذ فنی همراه است. از این گذشته، کسب اطلاعات مالی همواره برای ارتکاب جرم نیست و می‌تواند در راستای رقابت تجاری بین دو شرکت صورت بگیرد. حمله مهندسی اجتماعی و کسب اطلاعات مالی، غیر از اینکه دو اصطلاح فنی هستند تا حقوقی، چون با سایر عناوین مجرمانه پوشش داده می‌شوند، تحت عنوان مجرمانه مجزایی در قوانین کیفری انعکاس نیافته‌اند.

**ه) کلاهبرداری رایانه‌ای و دسترسی غیرمجاز به سیستم رایانه‌ای:**

نفوذ غیرمجاز مقدمه اکثر جرایم رایانه‌ای محسوب می‌شود و نسبت به کلاهبرداری رایانه‌ای در برخی مواقع در توسل به اقدامات مقدماتی برای تحصیل مال یا منافع دیگری ظاهر می‌شود. نفوذ کنندگان به سیستم رایانه‌ای چند قسم هستند.

هکرها کاوشگرانی هستند که از روی کنجکاوی یا مقتضیات فعالیت‌های رایانه‌ای خویش به سیستم نفوذ می‌کنند. هک ماهیتا نوعی دانش فنی است و جرم به شمار نمی‌رود.

کراکرها نفوذگران بدخواه هستند که از روی سوءنیت به سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرم‌های رایانه‌ای را منتشر می‌کنند، فایل‌ها را پاک کنند یا مرتکب سایر جرایم رایانه‌ای شوند. از کراکرها به کلاه سیاه‌ها نیز یاد می‌شود.

فریک‌ها نفوذگران به خطوط تلفن در فضای سایبر را گویند. این دسته از نفوذگران از طریق سیستم رایانه‌ای به سیستم ارتباطی و مخابراتی دست می‌یابند و آن را مورد استفاده قرار می‌دهند.

نفوذگران غیر حرفه‌ای، این دسته از نفوذگران به دو دسته به سیستم رایانه‌ای نفوذ پیدا می‌کنند؛ یا وارد قسمت‌هایی از سیستم می‌شوند که نیازی به دانش فنی قابل توجه ندارد و به پردازش ساده و آسان اتکا می‌کنند یا اینکه در مقام لاشه‌خوار پس از نفوذ یک هکر حرفه‌ای به دنبال وی وارد سیستم می‌شوند و اهداف و اغراض خود را محقق می‌سازند. (عالی پور، ۱۳۸۳)

**و) کلاهبرداری رایانه‌ای و ارسال نامه‌های الکترونیکی نامربوط:**

نامه‌های الکترونیکی ناخواسته یا اسپم‌ها، علی‌رغم اینکه به ظاهر کم اهمیت جلوه می‌کنند اما چون از یک سو دارای محتوای نامربوط بوده و به تعداد زیادی از کاربران ارسال می‌شود و از سوی دیگر سیل این پیام‌ها موجبات عصبانیت کاربران را فراهم می‌آورد، امنیت اطلاع‌رسانی رایانه و اینترنت و به ویژه حریم خصوصی افراد را تهدید می‌کند؛ و به همین دلیل کشورهای اروپایی در قبال جرم انگاری آن اقدامات جدی به عمل آورده‌اند.

هرچند اکثر کاربران نسبت به نامه‌های الکترونیکی ناخواسته، بی‌اعتنا هستند، اما چون غالب این نامه‌ها عمدتا درخواست کمک اضطراری یا وعده مسابقه یا جایزه کاذب است می‌تواند موجبات تحقق کلاهبرداری رایانه‌ای را فراهم سازد؛ و اصولا یکی از طرق صید قربانیان ناشناخته برای کلاهبرداری در فضای سایبر ارسال نامه‌های نامربوط به سایت‌های وب فریب دهنده است تا صدها نسخه پنهان از کلمات کلیدی متداول را به سایت‌ها بارگذاری کنند، حتی اگر کلمات ربطی به سایت وب نداشته باشند.

**نتیجه گیری و پیشنهادات**

به طور کلی، فناوری اطلاعات و اختصاصا فضای سایبر زمینه را برای ارتکاب برخی از جرائم مانند کلاهبرداری رایانه‌ای ساده‌تر ساخته است. این جرم به رغم ارتکاب آسان آن دارای ضرر

اقتصادی بیشتری نسبت به جامعه و افراد است که در اینصورت مجازات فعلی آن سبک بوده و راه های پیشگیری از این جرائم کافی به نظر نمیرسد. همان طور که جوامع با وقوع جرم در دنیای فیزیکی مقابله می‌کنند، ارائه راهکارهای مناسب در جهت مقابله و جلوگیری از وقوع جرم در محیط مجازی که از اوصاف و ویژگی‌های متفاوتی نسبت به محیط واقعی برخوردار است، امری ضروری است. علی رغم جرم انگاری شدن جرایم رایانه‌ای در حقوق داخلی ایران و همچنین وجود اسناد بین‌المللی مختلف از جمله کنوانسیون بوداپست در این زمینه، اما ارائه راهکارهای مقابله با جرایم رایانه‌ای بالاخص جرم کلاهبرداری رایانه‌ای در این قوانین و اسناد به چشم نمی‌خورد. بنابراین، تنظیم یک معاهده بین‌المللی با استفاده از تجارب ملی مورد پیشنهاد می‌گردد و در این صورت اراده سیاسی قوی و اجماع بین‌المللی به عنوان یک ضرورت مورد نیاز خواهد بود.

## منابع فارسی

### کتب

- **جرائم رایانه‌ای**(۱۳۸۳)، ترجمه: محمدعلی نوری و دیگران، چاپ اول، تهران، گنج دانش
- سالاری، مهدی(۱۳۸۶)، **کلاهبرداری و ارکان متشکله آن**، تهران، میزان، چاپ اول
- شامبیاتی، هوشنگ (۱۳۸۲)، **جرایم علیه اموال و مالکیت**(حقوق کیفری اختصاصی)، تهران، ژوبین، جلد دوم، چاپ ششم
- میر محمد صادقی، حسین (۱۳۹۴). **حقوق کیفری اختصاصی۲جرایم علیه اموال و مالکیت**، تهران، میزان

### خبرگزاری

- دزیانی، محمد حسن (۱۳۸۳)، **شروع جرایم کامپیوتری**، خبرنامه انفورماتیک، شماره ۹۳

### مقالات

- خرم آبادی، عبدالصمد (۱۳۸۶)، **کلاهبرداری رایانه‌ای از دیدگاه بین‌الملل و حقوق ایران**، فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی، شماره ۲، دوره ۳۷
- قناد، فاطمه(۱۳۸۷)، **کلاهبرداری الکترونیکی در بستر فناوری‌های اطلاعات ارتباطات**، مجله پژوهش و سیاست، شماره ۲۵
- عالی پور، حسن (۱۳۸۳)، **کلاهبرداری رایانه‌ای**، مجله پژوهش‌های حقوقی، شماره ۶
- زیبر، اولریش(۱۳۸۱)، **حرکت به سوی هزاره جدید مسئولیت در اینترنت**، ترجمه: محمد حسن دزیانی، خبرنامه انفورماتیک، شماره ۸۳، مرداد

## English Resources

### BooK

- Y Jewkes, M Yar (2013), **Handbook of internet crime**

### Site

- CR Baker (1999), **An analysis of fraud on the internet**, internet research
- Charlotte E.Bywell, Charles Oppenheim, (2001), **Fraud on Internet auction-s**, Aslib Proceedings,Vol. 53 Issue:7, https://doi.org/10.1108