دانشگاه جامع علمی کاربردی واحد بانک ملت استان اصفهان

پایان نامه کارشناسی رشته مدیریت امور شعب

موضوع

احراز هویت مشتریان در خدمات بانکی

استاد راهنما

جناب آقای مجید قدیری

استاد مشاور

سرکار خانم ذوالفقاری

نگارنده

سید محسن نوربخش

سال تحصیلی ۱۳۹۱-۱۳۹۰

بِسم اللہ الرحمن الرحیم

با تشکر از استاد عزیز جناب آقای قدیری معاون محترم فن آوری اطلاعات بانک ملت و همچنین سرکار خانم ذوالفقاری مسئول آموزش بانک ملت استان اصفهان که با رهنمودهای خود موجب ارائه بهتر این مجموعه شدند.

فهرست مطالب

پیشگفتار

سرقت ۲۰۰ میلیون تومانی در پی نقص سیستم احراز هویت بانک

در بررسی‌ها و انجام استعلامات لازم از بانک مربوطه، مشخص شد فردی با مدارک جعلی اقدام به افتتاح حساب دیگری کرده و کارت عابربانک و رمز دوم نیز دریافت کرده است و مبلغ ۱۶۰ میلیون تومان از طریق اینترنت به حساب پس انداز منتقل و با اعزام پیک موتوری و با تماس‌های تلفنی مبلغ را از طریق pos[1] به طلا فروشی پرداخت و مقداردو کیلوگرم شمش طلا خریداری کرده است. پیرو شکایت فردی مبنی بر برداشت غیرمجاز مبلغ ۲۰۰ میلیون تومان به صورت اینترنتی از حساب وی، مأموران اقدامات خود را آغاز کرده و مشخص شد مبلغ برداشت شده به حساب دیگری به نام شاکی در همان بانک واریز شده است و این در حالی است که شاکی عنوان کرد که فقط یک حساب در این بانک دارد.در تحقیقات بعدی که توسط کارشناسان پلیس فتا صورت پذیرفت، معلوم شد که متهم با شگرد خاصی به طوری که هویت وی نامشخص بماند از طلا فروشی خرید کرده است. پس از بررسی‌های نهایی و انجام تحقیقات روی تلفن همراه متهم و نیز خطوط اینترنتی فرد برداشت‌کننده، متهم شناسایی و دستگیر شد.

نکته تأمل‌برانگیز در این پرونده نقص‌عمده در سیستم احراز هویت، تحویل دادن رمز عبور و کارت عابربانک و رمزهای اینترنتی بانک به مشتریان است چرا که یک مشتری در صورت داشتن چندین حساب بانکی در شعب مختلف بانک و اخذ رمز اینترنتی تنها یکی از آن حساب‌ها قادر به دسترسی به تمام حساب‌های خود در دیگر شعب و جابجایی وجوه است که لازم است این نقص‌عمده توسط کلیه بانک‌ها و شعب رفع شود...

این تیتر یکی از روزنامه های کشور بود و سوالی که ممکن است در ذهن خودم و همکاران پیش آید این است که چگونه می توان از بروز چنین مشکلاتی جلوگیری کرد؟!

این تحقیق تلاش کوچکی است جهت آشنایی خوانندگان آن با مفهوم هویت و راه های احراز آن در سیستم بانکداری سنتی و الکترونیکی.

---

[1] دستگاه پایانه فروش یا کارتخوان (Point Of Service) دستگاهی است که از طریق ارتباط تلفنی یا شبکه‌ای به سیستم بانکی امکان انتقال خودکار مبلغ خرید از حساب فروشنده را فراهم می‌سازد. دستگاه‌های پایانه فروش علاوه بر امکان پرداخت دارای عملکردهای مختلفی از جمله پرداخت قبوض، شارژ سیم‌کارت، اعلام موجودی، دریافت صورتحساب، امکان انصراف از خرید و گزارش روزانه است که صاحبان آن را از مزایای شعبه کوچک بانکی برخوردار می‌کند.

مفهوم هویت

واژه هویت که در فارسی مورد استفاده قرار می گیرد، در اصل کلمه ای عربی (الهویه) است، این کلمه از «هو» یعنی «او» که ضمیر مفرد مذکر است، مشتق شده است. هویت عبارت است از فرایند معناسازی براساس یک ویژگی خاص یا مجموعه به هم پیوسته ای از ویژگی های خاص که بر منابع معنایی دیگر اولویت داده می شود. «گیدنز[۲]» در این باره می نویسد: «هویت، منابع معنا برای کنشگران است وبه دست آنها از رهگذر فرآیند فردیت بخشیدن ساخته می شود. با این حال ممکن است از نهادهای مسلط نیز ناشی شود، اما حتی در این صورت نیز هنگامی هویت خواهد بود که کنشگران اجتماعی آنها را درونی کنند و معنای آنها را حول این درونی سازی بیافرینند.» دو ویژگی را می توان برای هویت برشمرد: اول آن که هویت وجه تمایز میان «من» و «ما» با «دیگران» است؛ و دوم آن که هویت مهم ترین منبع شناخت، عواطف، احساسات و سازماندهی رفتارهای جمعی و فردی محسوب می شود. بنابراین، مفهوم **هویت ضرورتاً با دو امر متضاد تعریف می شود،** یعنی **همسانی و تفاوت**. این ادعا که چیزی یا فردی هویتی ویژه دارد، بدین معناست که این چیز یا فرد مانند دیگر وجودها، دارای آن هویت است و در عین حال چونان چیز یا فردی متمایز، هویت و خاصیتی دارد. به بیان روشن تر، هویت یعنی کیفیت یکسان بودن در ذات، ترکیب و ماهیت و نیز یکسان بودن در هر زمان و همه شرایط. در هر حال، هویت داشتن یا یگانه بودن، دارای دو جنبه متفاوت است: همانند دیگران بودن در طبقه خود و همانند خود بودن در گذر زمان. لذا هویت عبارت است از نیازهای روانی انسان و پیش نیاز هرگونه زندگی اجتماعی است .اگر محور و مبنای زندگی اجتماعی را برقراری ارتباط پایدار و معنادار با دیگران بدانیم، هویت اجتماعی چنین امکانی را فراهم می کند. به بیان دیگر، بدون تعیین چارچوبی برای هویت اجتماعی، افراد مانند دیگران خواهند بود و هیچ کدام از آنان نخواهند توانست به صورتی معنادار و پایدار با دیگران پیوند یابند.

---

[۲] آنتونی گیدنز (Anthony Giddens) از مشهورترین جامعه‌شناسان بریتانیایی است

هویت انسانی

هویت انسانی، مقوله‌ای اجتماعی است. همه انسانها به هنگام تولد، فارغ از اینکه در کجای زمین به دنیا می‌آیند و یا از چه تعلق قومی و قبیله‌ای برخوردارند، دارای ویژگی‌های یکسان نوع انسانی، در میان انواع موجودات زنده هستند و هیچ گونه تفاوت ماهوی با یکدیگر ندارند؛ بنابراین، مقوله هویت انسانی که در دوران رشد و تکوین انسان در جامعه شکل می‌گیرد، کاملا اجتماعی و جامعه شناسانه است و ربطی به خون و نژاد و رنگ پوست و ... ندارد.

مجموعه‌ای از خصوصیات مختلف فرد مانند ساختمان بدنی، خلق، رفتار، علایق، گرایش‌ها، توانایی‌ها و استعدادهای وی، و برآیند این مجموعه از ویژگی‌های آدمی . هویت در واقع، همان شخصیت است که مورد آگاهی درونی قرار گرفته است . احساس شخصیت را می‌توان هویت نامید . این نکته را باید مورد دقت قرار داد که شخصیت و هویت آدمی امری فراتر از شخصیت و هویت مکانیکی است، هویت آدمی وابسته به عناصر بی‌شماری است اما همه آن‌ها در پرتو نگاه و نگرش وی به خویشتن و جهان شکل می‌گیرد، تفسیری که فرد از خود و هستی تولید می‌کند سازنده هویت او خواهد بود.

از سوی دیگر، قوام هستی و شخصیت به معنی داری زندگی است، و معنی داری حیات و چگونگی آن در سایه نگاه، نگرش و تفسیر فرد از خود و هستی و اولویت گذاری‌های ارزشی شکل می‌یابد.

با توجه به این تعریف، باید بر دو نکته تاکید کرد:

هویت امری عقلانی و عاطفی است و تفسیری است؛ سنجیده و قانع کننده از شخصیت و ابعاد آن و هستی و معنای زندگی . هویت از یکسو امری درونی است و از سوی دیگر وابسته به عوامل فراوان بیرونی است که بر نگرش و تفسیر آدمی اثر می‌گذارد .

هویت در جامعه

هویت در طول تاریخ و در زمانها و مکان های گوناگون ویژگی های مختلفی داشته است .در یک جامعه سنتی هویت انسان ها بر آمده از یک نظام مقتدر سنت راهبردی و باورهای ثابت آئینی و اسطوره ای است. در چنین جامعه ای هویت افراد شامل ویژگی هایی همچون ثابت بودن، یکسان بودن، یکنواخت بودن و قابل پیش بینی بودند است. در این جوامع هویت همواره اجتماعی بوده و کمتر دیده شده که تردیدها و شک اندیشی های فردی در آن خللی وارد کند. هویت فردی اغلب ثابت و ایستا و بر تعریف مشخصی استوار بوده که از سوی اسطوره ها و نظام های قانونی و تعریف شده دیرینه پشتیبانی می شده است. در این نظام هر فرد بخشی از یک نظام خویشاوندی قدیمی است. اندیشه ها و رفتار او به چارچوبی معین محدود می شوند و سمت و سوی زندگی او کم و بیش مشخص است. از همین روست که پرسش و چون و چرایی درباره جایگاه و موقعیت انسان در جهان به میان آورده نمی شود.اما در مقابل در جوامع مدرن هویت ها در میان افراد متغیر بوده و متکی بر تفاوت آنهاست. در این جوامع ذهنیت افراد ثابت نیست، بلکه درگیر عدم پایداری هاست. هویت در جامعه مدرن خصلت شخصی و مدرن دارد اما در واقع امری اجتماعی و وابسته به مناسبات بین سازمانی است .

در عصر مدرن، هویت برای نخستین بار با بحران مواجه می شود. در این دوران هم مانند دوران سنتی، هویت فردی بر شالوده رابطه با دیگران استوار است، از ثباتی نسبی برخوردار است، اما تأثیر گذاری ها و تأثیرپذیری ها، سمت و سوی آن را چند وجهی می کند. در این دوران هر فرد چندین نقش اجتماعی را ایفا می کند و بنابراین می تواند هویت های متعددی را برای خود انتخاب کند. انسان این دوره، نگران آن بود که مبادا هویت اش گذرا و شکننده و یا کاذب باشد. در شرایطی این گونه، همواره یک خویشتن واقعی و فطری در زیر نقش هایی که انسان در اجتماع بازی می کند احساس می شد و تلاش فرد همه آن بود که این خویشتن واقعی را پیدا کند و دست کم در خلوت با آن روراست باشد.اما در دوره پست مدرنیته زندگی اجتماعی بسیار پیچیده تر از دوران مدرنیته است و گردش و شتاب بیشتری دارد. در این دوران گستره ای از هویت های گوناگون پیش روی انسان قرار دارد و اوباخواسته هاوآرزوهایی آشنایی یافته است که در گذشته با آنها بیگانه بود. جوامع به سرعت تکه پاره می شوند، انسان باید در فرصت ها و مجال های کوتاه، شماری از نقش هایی را که مدام بر دامنه و گستره آن افزوده می شود، به شکلی گذرا ایفا کند و همین واقعیت، برخورداری از یک هویت یکپارچه را دشوار و حتی ناممکن کرده است. در این دوره که با عناوینی همچون «عصر اطلاعات» و «عصر مجازی» مترادف شده فناوری های نوین اطلاعاتی و ارتباطی

و در رأس آنها شبکه عظیم جهانی اینترنت منابع متعدد و گوناگون هویتی را به افراد عرضه می کنند و زمینه بروز چالش های متعدد در هویت انسان امروزی را موجب می شوند.

هویت در عصر اینترنت

در عصر حاضر با ورود وسایل ارتباط جمعی از قبیل روزنامه،کتاب،تلویزیون، ماهواره و اینترنت زندگی انسان ها دستخوش تغییرات گسترده ای گردیده است .امروزه رسانه ها قادرند در یک پروسه شتابان، هویت های مجازی برای افراد و گروه ها درست کنند، بدون این که از مرزهای سیاسی مورد تجاوز نظامی قرار گیرند. از نتایج رشد شتابان فناوری های نوین ارتباطی می توان به بحران هویت در جوامع اشاره کرد. بحران هویت واژه ای است که برای توصیف عدم توانایی افراد در قبول نقشی که جامعه از آنها انتشار دارد به کار رفته است . جدی ترین بحرانی که یک شخص با آن مواجه می شود، در خلال شکل گیری هویت رخ می دهد.این بحران بدان جهت جدی است که عدم موفقیت در رویارویی با آن پیامدهای بسیاری دارد. در هنگامه بحران، کسی نمی داند هر آدمی واقعاً کیست و چه کاره است، چون در واقع چیزی مشخص نیست. امروز چیزی است و فردا چیز دیگر. همانند آدمی که کاملاً حس جهت یابی اش را از دست داده باشد، چند گامی به یک سمت برمی دارد و سپس در جهت دیگر و شاید هم در جهت مخالف جهت اول گام نهد .انسانی که دچار بحران هویت شده است به حال خود رها شده، به درون آشوب ها و نابسامانی های یک محیط ناب افتاده و در یک وضع حسرت بار فاقد هر نوع جهت یابی گرفتار شده است. در مجموعه گزارش هایی که به وسیله گروه نویسندگان و منتقدان طراز اول باشگاه معروف رم منتشر شده است به صراحت بحران مدرن به عنوان بزرگترین خطر زمینه ساز زوال فرهنگی و اخلاقی جهان امروز، تلقی شده است. آثار این بحران در تمام شئون زندگی کشورهای پیشرفته، در حال توسعه و عقب مانده به چشم می خورد .

از پیامدهای جدی و اساسی انقلاب ارتباطات و جامعه اطلاعاتی تحول در مفاهیم مکان و زمان و نیز چند منبعی هویت در عصر جدید است که هر یک به نوبه خود مفهوم هویت را دستخوش تغییر، ناپایداری و حتی بحران ساخته اند. فناوری های نوین ارتباطی مفهوم مکان و زمان را دستخوش تغییر کرده اند، در حالی که مکان و فضا از توانایی هویت سازی بسیار بالایی برخوردارند. به بیان روشن تر، مرزپذیری و قابل تحدید بودن مکان این امکان را فراهم می سازد که انسان ها با احساس متمایز بودن، ثبات داشتن و تعلق به گروه، امنیت و آرامش لازم را برای زندگی کسب کنند.در واقع، سه کار ویژه هویت آفرین مکان، بر خاصیت اصلی آن یعنی، مرزپذیری و ثابت بودن استوار است .

اما فناوری های نوین ارتباطی با از بین بردن مرزها، مکان ها و فضاها هویت افراد را دستخوش ناپایداری و بحران می سازند. از آنجا که مکان در مقایسه با فضا، توانایی و قابلیت بسیار بیشتری برای تأمین نیاز به ثبات، تمایز و همبستگی اجتماعی دارد، جامعه اطلاعاتی و شبکه ای با سرزمین زدایی و فضامند ساختن زندگی اجتماعی، نوعی ناپایداری، تزلزل و ثبات نداشتن در هویت و ذهنیت پدید می آورد.جامعه اطلاعاتی با تبدیل زمان تاریخی به حالت بی پایان، گذشته هویت بخش را نابود می کند. نابودی گذشته به معنای از میان رفتن خاطره و تاریخ، از میان رفتن پیوند میان گذشته مشترک و حال مشترک است. در چنین شرایطی انسان نوعی همزمانی را تجربه می کند و در دنیایی لحظه ای قرار می گیرد که در چارچوب آن گذشت زمان را نمی توان احساس کرد، در حالی که یکی از پیش نیازهای اصلی هویت، احساس تداوم در گذر زمان است و ذهنیت چونان آگاهی از زمان قلمداد می شود.بنابراین هنگامی که زمان چونان تداوم از میان می رود، وحدت سوژه هم مخدوش می شود و احساسی از موقتی بودن و متغیر بودن بر ذهن انسان چیرگی می یابد. فناوری های نوین ارتباطی در عصر ارتباطات نه تنها فرهنگ های گوناگون و پرشماری را در دسترس افراد و گروه های مختلف قرار می دهد، بلکه دنیاها و مرجع های اجتماعی آنان را افزون می سازد .

بنابراین، اندک و حتی واحد بودن مرجع های اجتماعی در جوامع سنتی که نیاز هویتی انسان ها به تعلق و همبستگی اجتماعی را به آسانی تأمین می کرد، از میان می رود و فرد ناگزیر می شود که با واحدهای اجتماعی کوچک و بزرگ مختلفی هویت پیدا کند. منابع و گزینه های هویتی که در چنین شرایطی عرضه می شوند، نه تنها متعدد و متنوع هستند، بلکه گاهی در تعارض با یکدیگر نیز قرار دارند. به این ترتیب، مرجع های اجتماعی و در نتیجه هویت ها نسبی می شوند. این نسبیت فراگیر، هویت سازی را به مسوولیت دشوار فردی و زندگی اجتماعی را به عرصه ای تعارض گونه تبدیل می کند.نسبی شدن فرهنگ ها نیز نوعی ناپایداری و ثبات نداشتن در هویت پدید می آورد.کنار هم قرار گرفتن فرهنگ های خاص در درون فضای اجتماعی بسیار گسترده و پهناور و نسبی شدن حاصل از آن، دنیایی فارغ از اصول عام و مطلق پدید می آورد و بنیادهای هرگونه یقین و قطعیت معناساز و هویت بخشی را متزلزل می سازد. این تزلزل، در واقع تزلزل پایه های ایمان و باور است. اما در جهت حفظ هویت فرهنگی باید راهبردهای متعددی از سوی مسوولان و برنامه ریزان اتخاذ شود. از جمله این راهبردها تقویت باورها، ارزش ها و نگرش های اصیل مذهبی و ملی است که از اصلی ترین عوامل حفظ هویت فرهنگی جامعه به شمار می رود .

ارزش های اصیل مذهبی و دینی به عنوان یک ابزار مهم در هویت بخشی به انسان ها و به ویژه نسل جوان و دادن معنا به زندگی و جهت بخشیدن به آن مطرح هستند، به طوری که «ساموئل هانتیگتون» نیز به نقش ارزشمند و والای

دین در حفظ هویت جوامع اشاره کرده و می نویسد: «دین به زندگی نخبگان نوپای جوامعی که در حال مدرن شدن هستند، جهت و معنا می دهد». آفرینش فرهنگی با اتکا به عناصر و مواریث فرهنگی غنی گذشتگان نیز یکی دیگر از راهکارهای حفظ هویت فرهنگی افراد است. بی شک چنانچه نسل جوان، از لحاظ فکری و فرهنگی پرمایه و غنی بوده و پایه های محکمی برای تفکر، جهان بینی و معنای زندگی داشته باشند، در برخورد با هجمه فرهنگی فناوری های نوین، معقولانه برخورد کرده و به درستی آنها را در ترکیب شخصیتی خود جذب می کند.

انقلاب ارتباطات در عصر حاضر تأثیرات شگرفی را در ابعاد مختلف زندگی انسان ها گذاشته است که از مهمترین آنها می توان به تأثیرات فناوری های نوین ارتباطی و اطلاعاتی بر فرهنگ ها اشاره کرد. فناوری های نوین و در رأس آنها شبکه جهانی اینترنت با دگرگونی در مفاهیم زمان و مکان، تغییر در اشکال نوین ارتباطی و ایجاد مراجع جدید هویت، موجب پیدایش ذهنیت های ناپایدار و هویت های جدید شده است.

در جوامع امروزی براثر تحولات ساختاری ناشی از این انقلاب، ذهنیت و هویت سیال و ناپایدار شکل می گیرد و برداشت انسان ها از مفاهیم مختلف زندگی دگرگون می شود.

انواع احراز هویت

احراز هویت اشخاصی که به نحوی با بانک و خدمات آن سرو کار دارند شامل موارد زیر می باشد :

اشخاص حقیقی، اشخاص حقوقی ، اتباع خارجی، وکلا ، ولی قهری، وصی که به دوصورت انجام می شود :

۱- حضوری

۲- غیر حضوری

○ مراجعه حضوری

مراجعه حضوری: عبارت است از مراجعه ارباب رجوع به شعب ، دفاتر یا ادارات مؤسسه اعتباری و مراوده با نیروی انسانی مؤسسه مذکور برای اخذ خدمت.

خدمات حضوری که مستلزم حضور در یکی از شعب بانک ها می باشد ؛ جهت افتتاح حساب ، واریز وجه نقد ، برداشت وجه نقد از حساب شخصی ، وصول چک و ...

○ مراجعه غیرحضوری

مراجعه غیرحضوری: عبارت است از مراجعه ارباب رجوع به انواع ابزارهای پذیرش و اخذ خدمت به واسطه ابزار شناسایی و بدون مراوده با نیروی انسانی مؤسسه اعتباری.

خدمات غیر حضوری پس از مراجعه به بانک افتتاح کننده حساب و فعال کردن آن نیازی به مراجعه حضوری به شعب بانک را ندارد و بعد از فعال شدن خدمات مشتری می تواند از آنها استفاده کند.

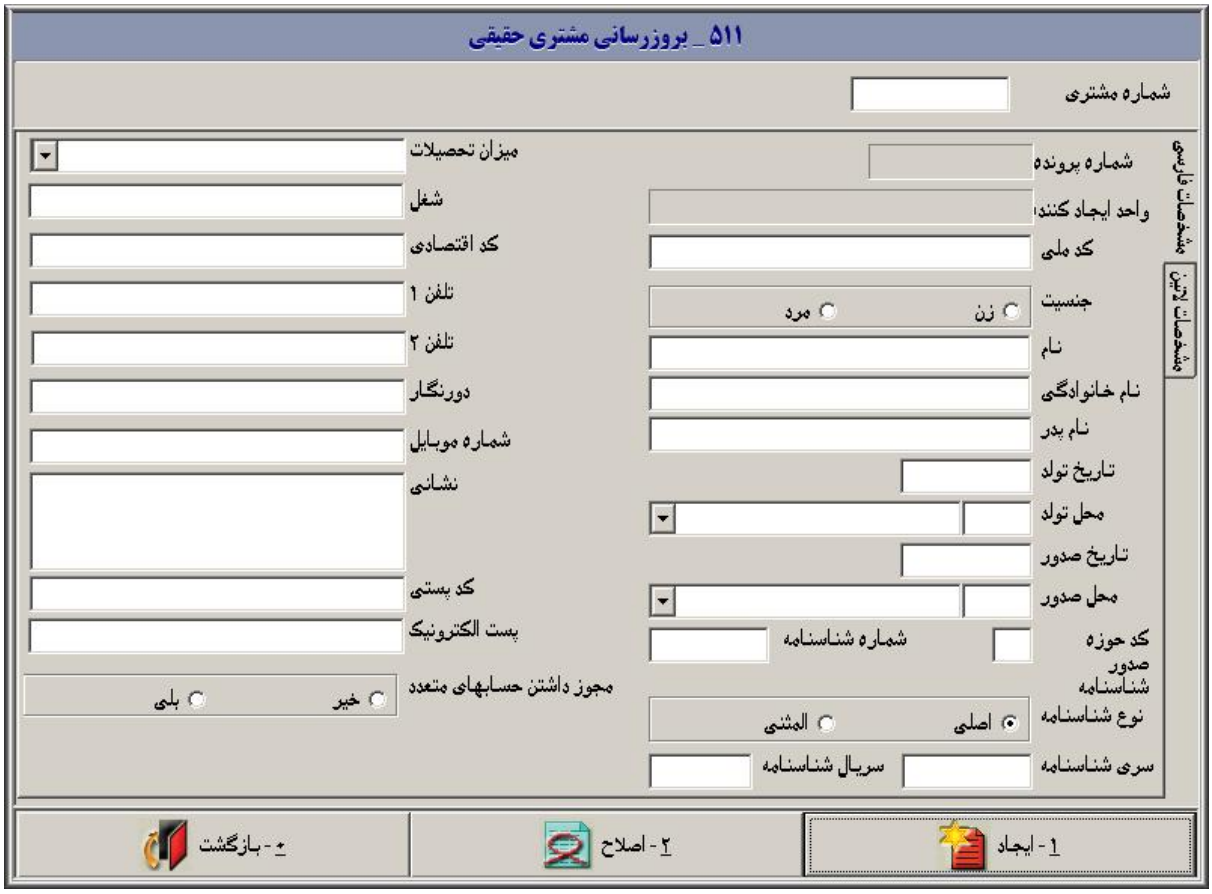
این خدمات شامل موارد زیر می باشند :

- همراه بانک
- تلفن بانک
- موبایل بانک
- بانکداری اینترنتی
- خودپرداز ها

- پایانه های فروش
- خرید اینترنتی
- انواع کارت های بانکی (اکسس، اعتباری ، هدیه و ...)

احراز هویت اشخاص حقیقی

هنگام مراجعه مشتریان جهت افتتاح حساب، با اطلاعات شناسنامه و کارت ملی و اطمینان به اطلاعات تماس پردازش ۵۱۱ انجام می شود و بعد از تایید صحت اطلاعات ، شماره مشتری ایجاد می شود و اطلاعات توسط سیستم جهت تایید به اداره ثبت ارسال می شود و ظرف مدت ۲۴ ساعت جواب آن به بانک میرسد.



ابزار احراز هویت افراد در هنگام مراجعه به شعب بانک ها ،کارت ملی که حاوی شماره ملی و کد پستی و عکس می باشد ؛ برای افتتاح حساب جاری تایید یک معرف معتمد بانک هم الزامی می باشد.

همچنین ارائه تصویر قبض تلفن ثابت و همراه جهت احراز کدپستی آخرین نشانی فرد در (طبق بخشنامه ۱/۲۲۹ مورخ ۸۸/۵/۲۴ اداره کل سازمان و بهبود روشها) حال حاضر الزامی است.

احراز هویت اشخاص حقوقی

در افتتاح حساب جاری برای شرکتها به دو نکته توجه می شود:

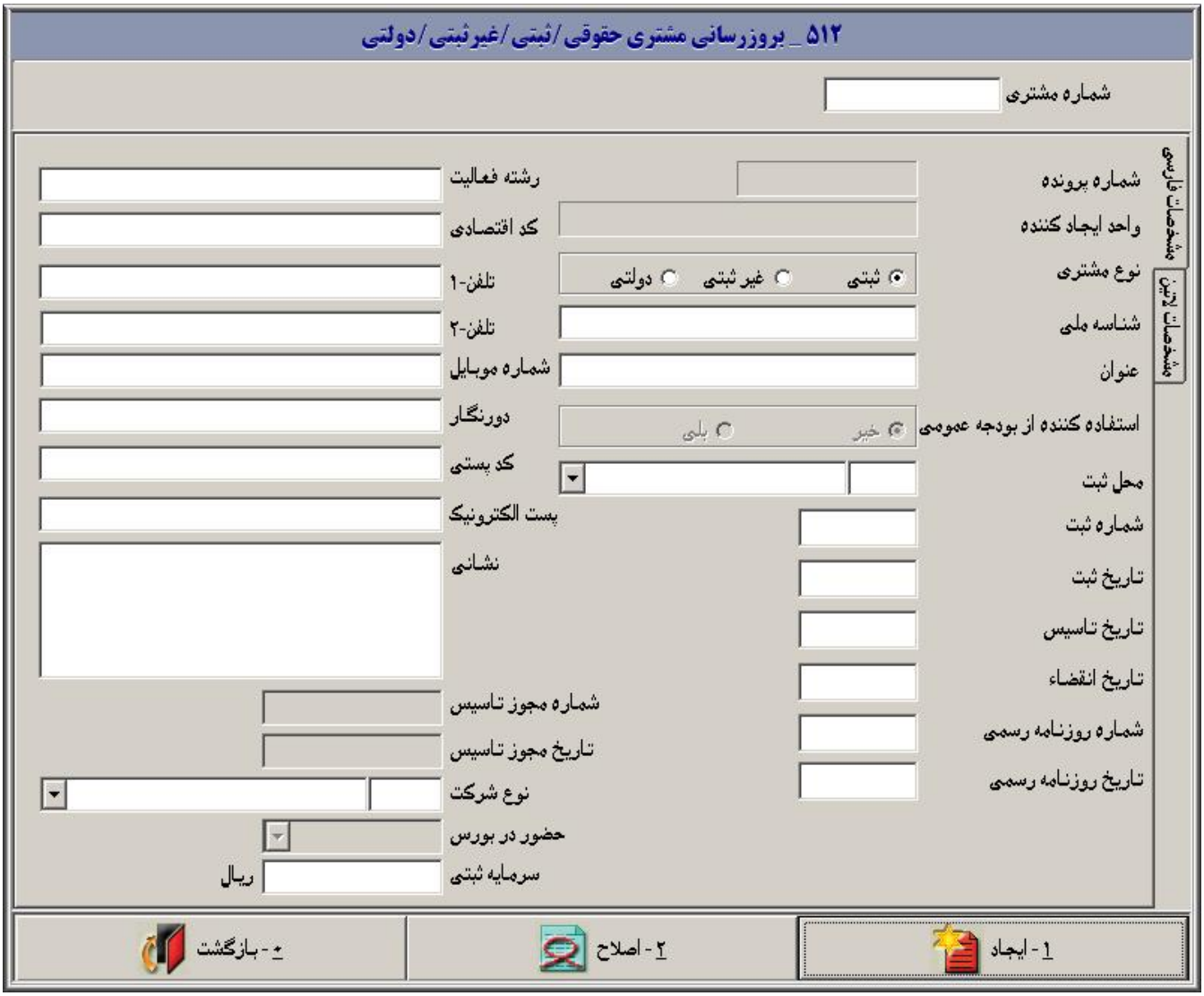
۱. شرکت های در شرف تاسیس

۲. شرکت های به ثبت رسیده

جهت ابراز هویت شرکت های در شرف تاسیس چون اطلاعاتی هنوز به ثبت نرسیده باید همچون اشخاص حقیقی اعمال کرد ولی به صورت اشتراکی.

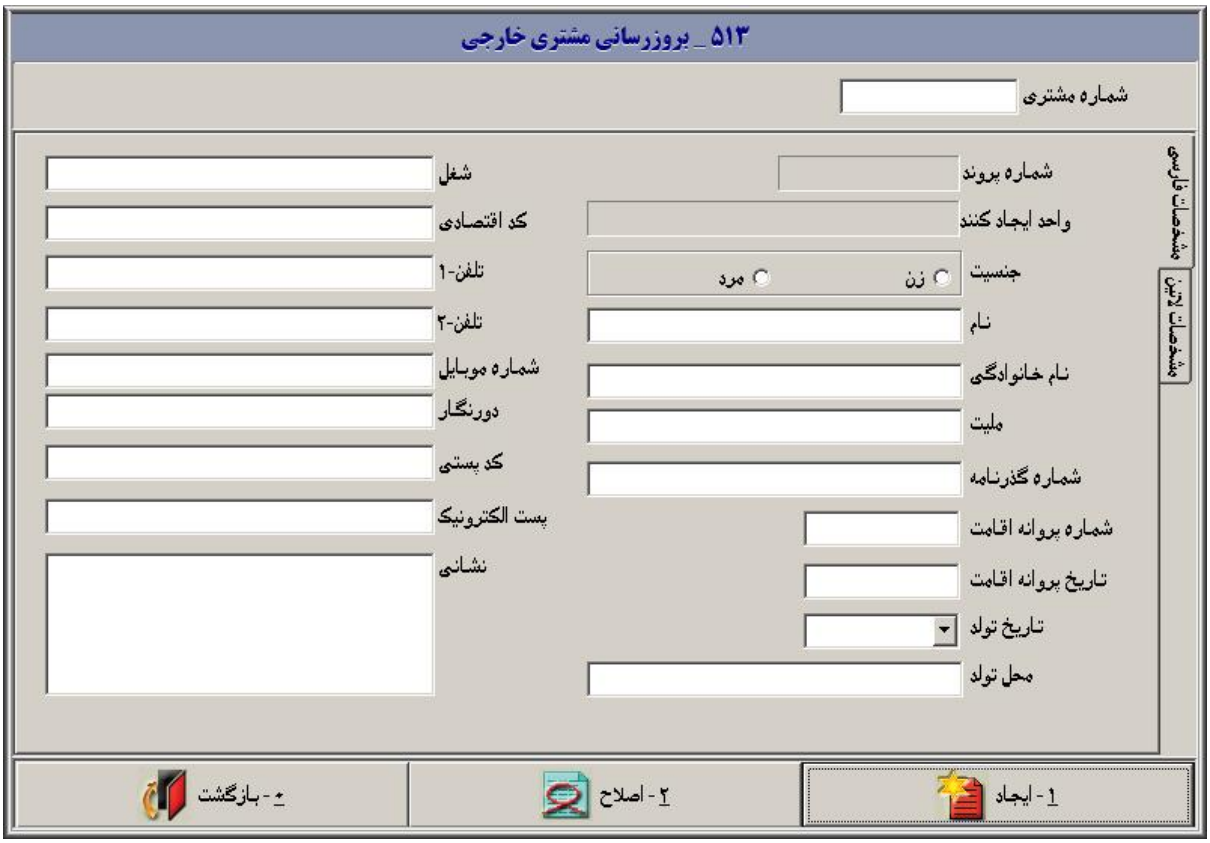
بعد از به ثبت رساندن شرکت مدارک زیر لازم می باشد:

- اساس نامه ، شرکت نامه (برای شرکت با مسئولیت محدود)، گواهی شده ثبت شرکتها
- روزنامه رسمی شرکت حاکی از ثبت شرکت و آخرین تغییرات حاصله در هیئت مدیره
- ارائه تصویر مالکیت یا اجاره نامه رسمی محل کسب و کار
- مدارک اشخاص حقیقی دارای مسئولیت و دارای امضا شرکت (در صورت تفویض اختیار به وکیل حتما باید در اساسنامه قید شده باشد)
- داشتن کد شناسه ملی که شبیه کد ملی است برای اشخاص حقوقی


۵۱۲ _ بروزرسانی مشتری حقوقی /ثبتی /غیرثبتی /دولتی
شماره مشتری
مشخصات فارسی
مشخصات لاتین
شماره پرونده
واحد ایجاد کننده
نوع مشتری
ثبتی
غیر ثبتی
دولتی
شناسه ملی
عنوان
استفاده کننده از بودجه عمومی
خیر
بلی
محل ثبت
شماره ثبت
تاریخ ثبت
تاریخ تاسیس
تاریخ انقضاء
شماره روزنامه رسمی
تاریخ روزنامه رسمی
رشته فعالیت
کد اقتصادی
تلفن-۱
تلفن-۲
شماره موبایل
دورنگار
کد پستی
پست الکترونیک
نشانی
شماره مجوز تاسیس
تاریخ مجوز تاسیس
نوع شرکت
حضور در بورس
سرمایه ثبتی
ریال
۱- ایجاد
۲- اصلاح
۰- بازگشت

احراز هویت اتباع خارجی (مطابق بخشنامه ۱/۲۲۹ مورخ ۸۸/۵/۲۴ اداره کل سازمان و بهبود روشها)

- دفترچه پناهندگی ،کارت ویژه هویت اتباع خارجی، آخرین برگ آمایش و گذرنامه
- معرفی سفارتخانه جهت افتتاح حساب جاری و داشتن گذرنامه
- پروانه اقامت دائم برای متقاضیان حساب جاری و پروانه اقامت موقت برای حساب قرض الحسنه
- توجه به شهرستان مجاز جهت تردد و افتتاح حساب فقط در آن شهر



احراز هویت وکیل و قیم

انواع وکالت نامه های مورد قبول بانک

۱ – وکالت نامه رسمی

وکالت نامه ایست که در دفاتر اسناد رسمی کشور تنظیم می شود . اگر بیش از سه سال از تاریخ تنظیم وکالت نامه سپری شده باشد بانک بایستی کتبا اعتبار آنرا از دفترخانه مربوط استعلام کند.

۲ – وکالت نامه بانکی

وکالت نامه چاپی موجود در بانک است که اختصاص به انواع امور بانکی مشتریان دارد و برای تنظیم آن باید موکل و وکیل هردو در شعبه بانک حضور یابند. در این وکالت نامه بایستی امضای وکیل و موکل به گواهی یکی از دفاتر اسناد رسمی برسد.

۳ – وکالت نامه کنسولی

این وکالت نامه در یکی از سفارتخانه ها یا کنسولگری های ایران در خارج از کشور تنظیم می شود .در ذیل آن امضای موکل بدون توجه به مفاد وکالت نامه گواهی شده و مهر سفارت در آن نقش می بندد. اعتبار این وکالت نامه ها ۳ سال و چنانچه مورد وکالت دریافت حقوق موکل باشد حداکثر یکسال است.(قبلا برای انجام مورد وکالت اینگونه وکالت نامه ها تائید مهر سفارت توسط وزارت امور خارجه و نیز تنفیذ وکالت نامه توسط دادگاه انقلاب اسلامی ضرورت داشت که در حال حاضر نیازی به تائید و تنفیذ مراجع فوق الذکر نیست.)

۴ – وکالت نامه زندانیان

این وکالت نامه بوسیله زندانی نوشته شده و در ذیل آن اثر انگشت زندانی توسط مسئولین زندان و با الصاق مهر زندان گواهی می شود.

چنانچه مورد وکالت اخذ تسهیلات بانکی و امضای قرارداد باشد ، اصلح است بدون توجه به تاریخ تنظیم وکالت نامه ، اعتبار آن استعلام گردد.

اخذ انواع تسهیلات بانکی به استثنای تسهیلات مضاربه می تواند موضوع وکالت نامه قراربگیرد.

قیم توسط قیم نامه[۳] معرفی می شود.

[۳] نامه ای که ازطرف مقام قضایی به قیم جهت قیمومت محجورین داده می شود .

احراز هویت جهت استفاده از خدمات غیر حضوری بانک

خدمات بانک ملت در حال حاضر شامل خدمات همراه بانک، تلفن بانک،اینترنت،پیامک بانک ،خود پرداز ،خرید اینترنتی و پابانه های فروشگاهی بانک ملت می باشد.

- همراه بانک : ابزار احراز هویت در خدمات همراه بانک ملت ، شماره تلفن همراه صاحب حساب است که در سیستم ثبت و به حساب متصل می شود به انضمام یک رمز و یک کلید تبادل که شامل یک کد جهت رمز نگاری (common key) به منظور جلوگیری از سرقت اطلاعات می باشد که اگر در صورت عدم دسترسی به موبایل رمز افشا گردد نمی توان از آن خدمات سوء استفاده کرد و یا در صورت مفقود شدن موبایل و نداشتن رمز ورود نمی توان به آن وارد شد.

- تلفن بانک : ابزار احراز هویت در تلفن بانک به صورت شماره حساب و رمز دریافت شده در شعبه افتتاح کننده حساب به صاحب حساب می باشد.

اگر با تلفن مجهز به سیستم Caller ID [۴] عملیات انجام شود ممکن است رمز روی صفحه نمایش باقی بماند و باعث پایین آمدن امنیت شود.

- اینترنت : ابزار احراز هویت در اینترنت شامل شناسه ای برای مشتری و یک رمز عبورمی باشد همچنین یک کد تصویری جهت جلوگیری از ارسال اطلاعات توسط ماشین AI[۵] . همچنین برای کسانی که بخواهند امنیت بیشتری برای جابجایی و برداشت از حساب کنترل شده داشته باشند می توانند از امضا الکترنیک استفاده کنند که شامل یک تراشه و یک ورودی درگاه USB [۶] و یک رمز ۸ رقمی می باشد.

---

[۴] Caller ID که در مکالمات فارسی به آن سرویس نمایشگر شماره تلفن می گوییم، طرفین یک ارتباط مخابراتی را قادر می سازد تا از شماره تماس گیرنده و مخاطب تماس آگاه شوند.

[۵] Artificial intelligence

[۶] Universal Serial Bus

- پیامک بانک : ابزار احراز هویت در پیامک بانک کمی شبیه به همراه بانک است با این تفاوت که احتیاج به هیچ برنامه خاصی نیست و فقط از طریق پیامک می توان آن را ارسال نمود و خدمات جابجایی پول ندارد.
- خودپرداز :در ابزار احراز هویت در خودپرداز می توان به داشتن اصل کارت (کارت فعال و متصل به حساب) و همچنین رمز ورود اشاره کرد که بعد از ورود با رمز می توان رمز دوم و کد cvv2[۷] و تاریخ انقضا کارت را دریافت کرده جهت خدمات اینترنتی از آن استفاده نمود.

- خرید اینترنتی :در ابزار احراز هویت در خرید اینترنتی می توان به شماره روی کارت و cvv2 و تاریخ انقضا و رمز اینترنتی یا رمز دوم کارت اشاره کرد . برای بالا بردن امنیت اطلاعات باید از پروتکل های https و ssl استفاده کرد .

- خرید با استفاده پایانه فروشگاهی :ابزار احراز هویت در خرید از دستگاه پایانه فروش فقط اصل کارت و رمز کارت همانند دستگاه خودپرداز است در صورتی که اگر از کارت ملی یا کارت شناسایی استفاده شود امنیت آن بالا میرود که شاید توقعی بیجا باشد زیرا فروشنده فقط قصد فروش محصول را دارد نه حفاظت از منافع مردم

[۷] Card Verification Value II – شماره شناسایی دوم مشتری می باشد که دارای سه رقم بوده و در پشت کارت های صادره بانک ملت نیز چاپ می شود.

پروتکل های Https و SSL

SSL [۸] راه‌حلی جهت برقراری ارتباطات ایمن میان یک سرویس‌دهنده و یک سرویس‌گیرنده است که توسط شرکت Netscape ارایه شده است. در واقع SSL پروتکلی است که پایین‌تر از لایه کاربرد (لایه ۴ از مدل TCP/IP[۹]) و بالاتر از لایه انتقال[۱۰] (لایه سوم از مدل TCP/IP) قرار می‌گیرد. مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل‌های غیرامن لایه کاربردی[۱۱] نظیر HTTP[۱۲] ، LDAP[۱۳] ، IMAP[۱۴] و... می‌باشد که براساس آن الگوریتم‌های رمزنگاری بر روی داده‌های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول کانال انتقال تضمین می‌کند.

به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس‌دهنده و سرویس‌گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند، البته غیر از این‌کار می‌بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این‌کار را با کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می‌دهد.

---

[۸] Secure Socket Layer

[۹] Transmission Control Protocol/Internet Protocol

[۱۰] Transport Layer

[۱۱] Application layer

[۱۲] Hypertext Transfer Protocol

[۱۳] Lightweight Directory Access Protocol

[۱۴] Internet message access protocol

مکانیزم‌های تشکیل‌دهنده SSL

۱- تأیید هویت سرویس‌دهنده

با استفاده از این ویژگی در SSL، یک کاربر از صحت هویت یک سرویس‌دهنده مطمئن می‌شود. نرم‌افزارهای مبتنی بر SSL سمت سرویس‌گیرنده (مثلاً یک مرورگر وب نظیرInternet Explerer از تکنیک‌های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس‌دهنده (مثلاً یک برنامه سرویس‌دهنده وب نظیر IIS[۱۵]) می‌تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می‌تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت‌های اعتباری و یا گذرواژه‌ها اقدام نماید.

۲- تأیید هویت سرویس‌گیرنده

برعکس حالت قبلی در اینجا سرویس‌دهنده است که می‌بایست از صحت هویت سرویس‌گیرنده اطمینان یابد. طی این مکانیزم، نرم‌افزار مبتنی بر SSL سمت سرویس‌دهنده پس از مقایسه نام سرویس‌گیرنده با نام‌های مجاز موجود در لیست سرویس‌گیرنده‌های مجاز که در داخل سرویس‌دهنده تعریف می‌شود و در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می‌دهد.

۳- ارتباطات رمز شده

کلیه اطلاعات مبادله شده میان سرویس‌دهنده و گیرنده می‌بایست توسط نرم‌افزارهای موجود در سمت سرویس‌دهنده و سرویس‌گیرنده رمزنگاری[۱۶] شده و در طرف مقابل رمزگشایی [۱۷] شوند تا حداکثر محرمانگی [۱۸] در این‌گونه سیستم‌ها لحاظ شود.

---

[۱۵] Internet Information Services

[۱۶] Encrypt

[۱۷] Decrypt

[۱۸] Confidentiality

حملات تأثیرگذار برSSL

SSL نیز از حملات و نفوذهای مختلف در امان نیست. بعضی از حملات متداولی که براین پروتکل واقع می‌شود عبارتند از: Traffic Analysis[۱۹] ، حملات Paste Cut بلووین، حملات Certification Injection و حملات از نوع Man in the middle.

پروتکل Https[۲۰]

انتقال اطلاعات در اینترنت، از طریق پروتکل‌های مختلف انجام می‌شود که استفاده از آن بستگی به نیاز کاربر و سرور مربوط به این پروتکل دارد. دو نمونه از پروتکل‌های رایج Http و Https هستند.

لغت "S" در Https مخفف کلمه secure است به عنوان مثال هنگام ورود به سایت بانک‌ها، ارسال فرم‌های online ، ایجاد حساب کاربری، خریدهای اینترنتی و یا در صورت نیاز به هر گونه انتقال اطلاعات امن در محیط وب از پروتکل https استفاده می‌شود. این پروتکل تمام اطلاعات رد و بدل شده بین شما و سایت را به صورت رمزگذاری شده رد و بدل می‌کند که در بین راه برای دیگران قابل خواندن نخواهد بود .HTTP ، پروتکل امن انتقال اطلاعات ابر متن هاست[۲۱] که برای انتقال اطلاعات رمز گذاری شده میان کامپیوترها از راه اینترنت به کار می رود. HTTPS همان HTTP است که از یک SSL استفاده می کند. SSL پروتکل رمز گذاری است که در وب سروری که از HTTPS استفاده می کند به کار گرفته می شود. یکی از دلایل مهم استفاده از HTTPS انجام خرید آن لاین و مبادله اطلاعات خصوصی از طریق اینترنت است.

---

[۱۹] تحلیل ترافیک

[۲۰] Hypertext Transfer Protocol Secure

[۲۱] HTTP

روش‌های احراز هویت

- اطلاعات سجلی و پایه ای افراد :

استعلام از سازمان های ثبت احوال ، بانک مرکزی ، ادارات و سازمانهایی که به نحوی با احراز هویت افراد در ارتباط هستند و اطلاعات آنها می تواند به یکدیگر کمک کند، سامانه فرانام و استعلام online.

- چیزی که کاربر بداند :

رمز عبور متنی ، رمز عبور تصویری

- چیزی که کاربر مالک آن است :

توکن‌های امنیتی ، کارت‌های هوشمند و RFID

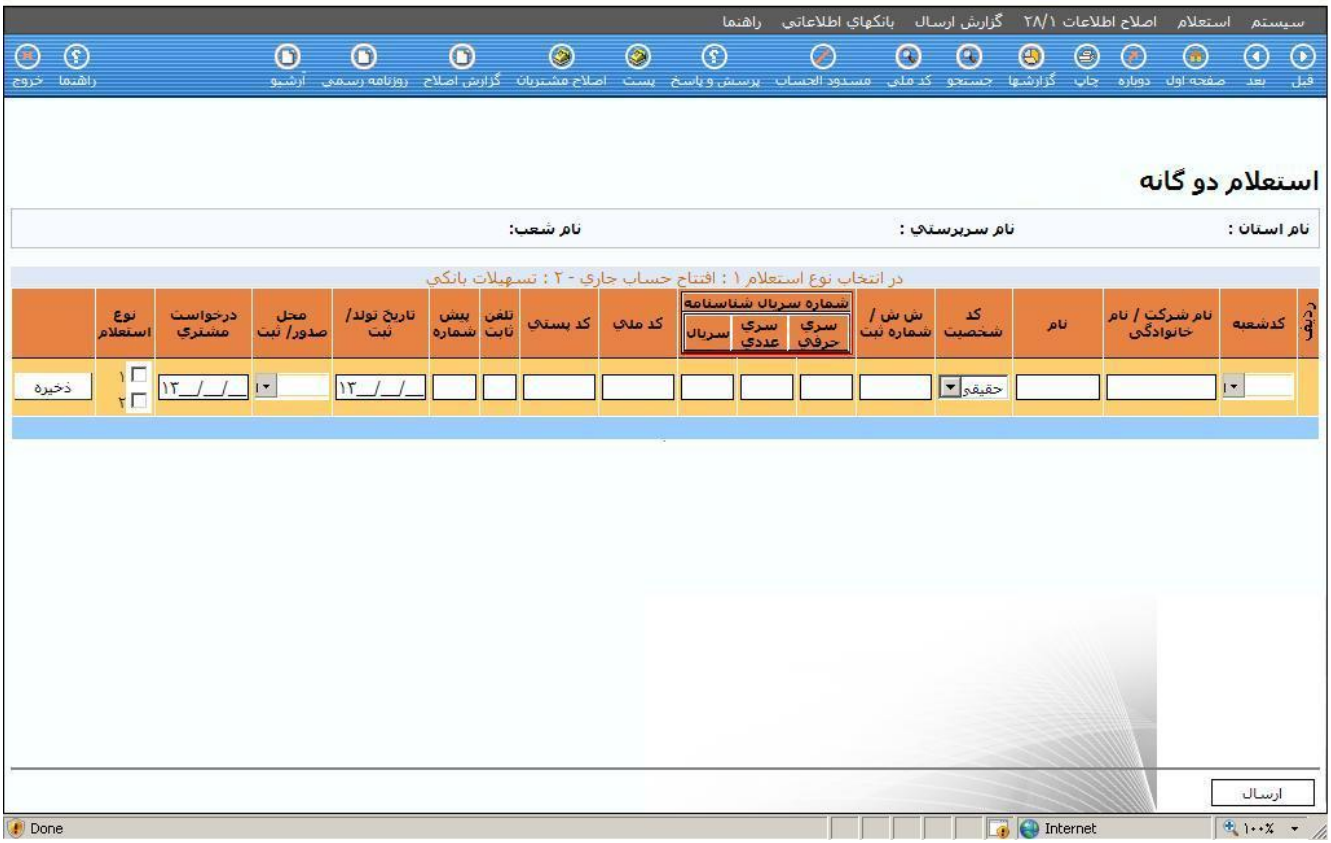
- چیزی که کاربر از نظر بیولوژیک دارد (کنترل بیومتریک) :

اثر انگشت ، الگوی شبکه چشم ، تشخیص چهره ، تشخیص صدا

استعلام

استعلام یعنی در خواست شناسایی از مرجع ذیصلاحی که می تواند اطلاعاتی که مد نظر ما است را برای ما تایید یا رد کند این اطلاعات می تواند اطلاعات و مشخصات سجلی افراد باشد همچنین اطلاعات و سوابق مالی اشخاص یا اطلاعات محل سکونت یا اطلاعات اموال و دارایی و یا روابط مالی موجود بین اشخاص که می تواند مثمر ثمر باشد در سال ۱۳۸۶ بانک ملت با همکاری سازمان ثبت و احوال کشورموفق به استعلام مشخصات سجلی افراد به صورت offline شد و در حال حاضر بانک ملت این استعلام را بصورت online انجام می دهد .

در ضمن با استفاده از سامانه فرانام می توان نسبت به استعلام افتتاح حساب بانکی و تسهیلات بانکی و تعهدات ارزی اقدام کرد برای استفاده از این سامانه باید از یک مرورگر اینترنتی استفاده کرد همچنین رمز عبوری که مخصوص به هر شعبه می باشد ؛ بعد از ورود می توان از منوهای آن جهت ورود اطلاعات استفاده کرد که شکل آن را در تصویر زیر می بینید :



رمز عبور متنی

رمزهای عبور بخش مهمی از سرویس های بانکی الکترونیکی می باشند و در حقیقت در خط مقدم حفاظت از حساب های کاربری در سرویس های مذکور قرار می گیرند. این کلمات عبور شامل حروف ، اعداد و علائمی است که هر کدام به صورت یک کاراکتر می باشد یک کلمه عبور نامناسب ممکن است منجر به کلاه برداری های مالی بزرگی شود.بهترین رمز عبور، رمزی است که شما آن را به راحتی به خاطر می سپارید ولی دیگران نمی توانند آن را حدس بزنند.

وقتی که رمز عبور خود را انتخاب کردید آن را به طور منظم عوض نمایید. اگر برای یک سال است که از یک رمز عبور استفاده می کنید الان زمانی است که باید آن را تغییر دهید.هرگز رمز عبور خود را در اختیار دیگران نگذارید و هیچ گاه آن را جایی ننویسید یا در کامپیوتر خود ذخیره نکنید.

در انتخاب رمز عبور مناسب به موارد زیر دقت کنید:

- هیچ گاه برای رمز عبور خود از اطلاعات شخصی مانند اسم، تاریخ تولد، شماره موبایل و ... استفاده نکنید.
- رمزهای عبور پیش فرض را پس از اولین ورود به سیستم تغییر دهید.
- بهتر است رمزهای عبور در سیستم های مختلف با یکدیگر متفاوت باشند.
- هر چقدر رمز عبور طولانی تر باشد امنیت آن بیشتر است (حداقل ۸ کاراکتر.)
- از رمز های عبور ترکیبی استفاده کنید که شامل حروف کوچک، حروف بزرگ، ارقام و نشانه ها شود.
- سعی کنید در رمز عبور حداقل یک بار ازکلید Space استفاده نمایید.
- حداقل هر ۳ ماه یک بار بنا به دفعات استفاده، رمز عبور خود را تعویض کنید که البته تغییر یک ماهه توصیه می شود.
- کلمات عبور خود را با هیچ کس درمیان نگذارید. با تمام رمزهای عبور خود به عنوان اطلاعات حساس محرمانه برخورد کنید.

امنیت در بانکداری الکترونیک

منظور از امنیت، حفاظت داده‌ها درمقابل افراد غیرمجاز و خاطی در فرآیند تجارت الکترونیک می‌باشد اینترنت یک شبکه کاملاً باز است و تا هنگامی که تدابیر لازم جهت عدم امکان دسترسی اشخاص غیرمجاز به‌منظور دراختیار قرار گرفتن اطلاعات و مداخله در آنها پیش‌بینی نگردد اطلاعات می‌تواند مورد دستبرد یا دستکاری قرار گیرد.
برای مثال زمانی که از کارت اعتباری در خرید استفاده می‌گردد چنانچه شمارت کارت اعتباری دراختیار افراد غیرمجاز قرارگیرد با سوءاستفاده از آن ممکن است خسارات مالی به صاحب کارت وارد آید و این خود دلیل آشکاری است برای محافظت هرچه بیشتر از تعاملات الکترونیکی[۲۲] در شبکه اینترنت .

ابزارهای اصلی این مراقبت رمزنگاری[۲۳] و شناسایی هویت[۲۴] می‌باشد.

[۲۲] transactions
[۲۳] Encryption
[۲۴] Authentication

هویت شناسی

باید توجه داشت در فرآیندهای تجارت الکترونیکی حتی اگر مکانیزم‌های رمزگذاری و رمزگشایی مورد استفاده قرار گیرند هنوز هم می‌باید مشکلاتی را که می‌تواند به‌سبب استفاده غیرمجاز اشخاص به‌وجود آید را درمدنظر داشت.برای مثال شخصی غیرمجاز می‌تواند خود را اپراتور فروشگاه معرفی نماید و از خریداران بخواهد تا مبالغ صورتحساب‌های خود را به حساب او واریز نمایند بدون آنکه عملاً کالاهای سفارش‌شده را دراختیار خریداران قرار دهد و همچنین ممکن است فردی غیرمجاز با استفاده از مشخصات شخص دیگری اقدام به صدور سفارش نماید بدون آنکه مبالغ سفارش سفارش خود را پرداخت نموده باشد. در اینترنت بصورت فیزیکی دوطرف یکدیگر را مشاهده نمی‌نمایند و اصولاً فروشگاه‌ها بصورت غیرفیزیکی و مجازی می‌باشند به همین خاطر روشهای مختلفی عرضه گردیده است تا هویت طرف مقابل را تأیید نماید. اینگونه شناسایی‌ها می‌تواند ازطریق ارائه کلمه عبور، اثر انگشت، امضاهای دستی و یا نظایر آن انجام پذیرد.

مؤسسات Certification Authority

در یک شبکه باز مانند اینترنت، درنظرگرفتن تمهیداتی درمقابل تهدیدات، حیاتی است، تهدیداتی مانند جعل هویت، تحریف و درزکردن اطلاعات.بنا به تعریف، در فرآیندها کسب و کار الکترونیک هویت شناسی درواقع جلوگیری از جعل هویت طرفین معامله توسط افراد غیرمجاز می‌باشد. لذا به‌منظور حصول اطمینان از هویت طرفین معامله در یک تعامل یا فرآیند تجاری (transaction) و تأیید یا رد صلاحیت آنها، نیاز به ایجاد مؤسساتی است که این وظیفه را به‌عهده گیرند. این مؤسسات موسوم به CA[۲۵] می‌باشند.

ازآنجایی که گواهی صادره توسط CAدر تعاملات فیمابین دوطرف معامله تجاری از اهمیت ویژه‌ای برخوردار است، لذا نه‌تنها گواهی صادره می‌باید ازنظر صحت و یا عدم جعل آن تدابیر لازم را رعایت نماید، بلکه برای صدور این گواهینامه نیز می‌باید رویه‌های خاص و فرآیندهای ویژه‌ای را درنظر گرفت. ازاین‌رو لازم است مؤسسات فوق‌الذکر از حسن اعتبار و بنیه اقتصادی و توان فنی بالایی برخوردار باشند.به‌منظور ارائه استانداردهای لازم درمورد مؤسسات CA مؤسسه بین‌المللی ISO با تشکیل کمیته‌ای تخصصی، استانداردی به‌نام **X ۹۰۵** را تدوین و اعلام نموده است.هر گواهینامه دارای یک امضای CA است. این امضا مبین آن است که شخص شرکت‌کننده در فرآیند تجاری و تعاملات الکترونیکی صاحب قانونی کلید public مورد استفاده می‌باشد.

[۲۵] Certification Authority

رمزنگاری (Encryption)

استفاده از کلیدها جهت رمزگذاری و رمزگشایی Encryption گفته می‌شود. معمول‌ترین شیوه جهت محافظت و امنیت داده‌ها روش رمزنگاری می‌باشد. در این روش اطلاعات با استفاده از یک کلید رمزشده و ازطریق اینترنت ارسال می‌گردند و در طرف دیگر، گیرنده اطلاعات نیز ازطریق یک کلید آنها را رمزگشایی نموده و می‌خواند.

شخص ثالثی که فاقد کلید مربوطه باشد حتی درصورت دراختیار داشتن اطلاعات رمزشده، نمی‌تواند اطلاعات را بخواند. دو سیستم رمزنگاری موسوم به Common key و Public key وجود دارد. امروزه این دو سیستم را نیز توأماً مورد استفاده قرار می‌دهند.یکی از متداولترین رویه‌های رمزنگاری ازطریق Public key موسوم به رمزنگاری RSA می‌باشد.

RSA[۲۶] یک سیستم رمزنگاری و شناسایی هویت در اینترنت است که به‌عنوان یک الگوریتم در سال ۱۹۷۷ توسط سه‌نفر به‌نام‌های Ron Rivest ، Adi Shamir و Leonard Adleman ایجادگردیده است.

این الگوریتم معمولترین الگوریتم در رمزنگاری و شناسایی هویت به‌عنوان بخشی از وب به مرورگرهای Netscapeو IE - Micersoft افزوده شده است. ضمن آنکه این الگوریتم به‌عنوان بخشی از محصولات Lotus Notes Intuist,s Quicken و بسیاری از محصولات دیگر به‌حساب می‌آید.

[۲۶] Rivest-Shamir-Adleman

رویه رمزنگاری به روش Common Key

در این روش رمزگذاری و رمزگشایی یک پیام به‌گونه‌ای است که هر دو طرف گیرنده و فرستنده از کلید مشابهی استفاده می‌کنند. فرستنده اطلاعات با استفاده از یک کلید اختصاصی (Private) اطلاعات را ارسال و شخص گیرنده اطلاعات ازطریق اینترنت با استفاده از همان کلید اختصاصی، متن رمزگذاری‌شده را به‌حالت اولیه برمی‌گرداند. در این سیستم هر دو طرف گیرنده و دریافت‌کننده می‌باید ازقبل این کلید رمز یکسان را بدانند . دراختیار قراردادن کلید مشترک توسط public key cryptographic scheme و ازطریق اینترنت انجام می‌پذیرد.

رویه رمزنگاری به‌روشPublic key

بکارگیری این روش برای خریدارهای online امنیت کاملی را تضمین می‌نماید. این روش در حال حاضر معمولترین روش استفاده از تکنیک‌های رمزگذاری در اینترنت می‌باشد. در این روش کاربران دو کلید عمومی (Public) و خصوصی (Private) را توأماً جهت رمزگذاری و رمزگشایی پیام‌ها مورد استفاده قرار می‌دهند. به‌عنوان مثال یک فروشگاه مجازی مبتنی‌بر اینترنت کلید عمومی خود را دراختیار مشتریانش قرار می‌دهد و مشتریان با استفاده از کلید مذکور اطلاعات مربوط به سفارشات خود را رمزگذاری و به فروشگاه ارسال می‌نمایند. سپس فروشگاه پس از دریافت آنها با کلید خصوصی خود اقدام به رمزگشایی می‌نماید. بدین ترتیب محیط مطمئن‌تری فراهم می‌گردد.

این شیوه جهت الحاق امضای الکترونیکی همراه سفارش نیز می‌تواند مورد استفاده قرار گیرد.

کارتهای هوشمند غیر تماسی

در دهه ۱۹۷۰ میلادی برای اولین بار ایده استفاده ازکارت‌های هوشمند مطرح شد و از اواخر ۱۹۸۰ میلادی کارت‌های مغناطیسی که دارای یک نوار مغناطیسی با ظرفیت ذخیره‌سازی پایینی بودند به طور عملی وکاربردی وارد نظام بانکی کشورهای جهان گردید. بعدها نوع الکترونیکی کارت‌های هوشمند عرضه شد که دارای یک ریزتراشه[۲۷] برای نقل و انتقال و پردازش اطلاعات بود و توانایی ذخیره سازی بالاتری را داشت. کارتهای هوشمند مورد استفاده در نظام بانکی ایران عمدتا از نوع کارت‌های تماسی بوده و از سیستم مغناطیسی یا بعضاً الکترونیکی استفاده می نمایند که جهت پردازش و انجام عملیات مورد نظر تماس مستقیم کارت با دستگاه کارت خوان الزامی است. کارت هوشمند غیر تماسی با به کارگیری تکنولوژی RFID بدون نیاز به تماس مستقیم می توانند تمام وظایف کارت‌های مغناطیسی و الکترونیکی را انجام دهند، ضمن اینکه از آسیب پذیری کمتری نیز برخوردار هستند.

کارت‌های هوشمند متداول به طور معمول می توانند در موارد زیر مورد استفاده قرار گیرند:

- کارتهای ATM
- کارتهای بدهی
- کارتهای هزینه
- کارتهای اعتباری

به کارگیری تمام موارد فوق با استفاده از کارت‌های هوشمند غیر تماسی مجهز به تکنولوژی امواج رادیویی نیز امکان‌پذیر می باشد. مزیت عمده کارت‌های بدون تماس نسبت به کارت‌های مغناطیسی و کارت‌های دارای تراشه الکترونیکی معمول، سرعت بالاتر و امنیت بیشتر آنهاست. به طور کلی مزایای استفاده از تکنولوژی امواج رادیویی درکارت‌های غیر تماسی به شرح زیر است:

---

[۲۷] Micro Processor

- تسریع در انجام امور
- امنیت بالاتر
- هزینه کمتر نگهداری قرائتگرها
- عدم نیاز به تعویض مکرر کارت‌های فرسوده شده
- افزایش توانایی سرویس دهی در اماکن پر ازدحام
- امکان تولید کارت‌ها با اشکال مختلف

سیستم RFID

شناسایی با استفاده از فرکانس رادیویی Radio Frequency Identification که به اختصار آن را RFID می‌گویند یک عبارت کلی است برای تشریح سیستمی که هویت (در قالب یک شماره سریال منحصر به فرد) یک شیء یا انسان را از راه دور با استفاده از امواج رادیویی ارسال می‌کند. این سیستم بخشی از تکنولوژی‌های خودکار شناسایی است.

تکنولوژی‌های خودکار شناسایی یا Auto - ID Technologies شامل بارکدها، دستگاه رمزخوان اپتیکال و برخی از تکنولوژی‌های زیست‌سنجی[۲۸] از جمله اسکنرهای قرنیه چشم می‌شود. از این تکنولوژی‌ها در جهت کاهش زمان و نیروی انسانی لازم برای وارد کردن اطلاعات به صورت دستی و افزایش دقت اطلاعات استفاده می‌شود.

یک لیبل RFID رایج از ریزتراشه [۲۹] ، یک آنتن رادیویی و یک سطح چاپ‌پذیر تشکیل شده است. ریزتراشه به آنتن وصل است و آنتن نیز روی سطح چاپ‌پذیر نصب شده است. این ریزتراشه قادر است تا ۲ کیلوبایت اطلاعات در خود ذخیره کند. این اطلاعات می‌توانند شامل یک محصول خاص یا تاریخ ارسال آن، تاریخ ساخت، مقصد و تاریخ فروش محصول باشند. برای برداشت اطلاعاتی که روی ID لیبل وجود دارد به یک دستگاه کدخوان یا Reader نیاز است. یک دستگاه کدخوان رایج دارای یک یا دو آنتن است که امواج رادیویی را ارسال و سیگنال‌هایی که از لیبل فرستاده می‌شود دریافت می‌کند.

بیش از یک دهه است که تکنولوژی RFID توسط هزاران شرکت مورد استفاده قرار گرفته است. کاربردهای تجاری و بازرگانی RFID برخی از شیوه‌هایی را که در این تکنولوژی تاکنون مورد استفاده قرار گرفته و در آینده نیز مورد استفاده قرار خواهد داد، تعیین می‌کند. این تکنولوژی جدید نیست پس چرا پس از یک دهه تازه مورد استقبال قرار گرفته است؟

تاکنون هزینه بالای RFID استفاده از آن را محدود می‌کرد. برای بسیاری از کاربردها مثل ردیابی قطعات برای تولید لحظه‌ای و براساس نیاز(Just in Time) هزینه لیبل‌های RFID که بیش از یک دلار برای هر لیبل است توجیه‌پذیر بود. زیرا صرفه‌جویی که برای سازندگان به ارمغان می‌آورد بیش از هزینه آن بود. از سوی دیگر هنگامی که RFID برای ردیابی موجودی یا ظروف بسته‌بندی در چهاردیواری یک شرکت به‌کار گرفته می‌شود، لیبل‌ها

---

[۲۸] Biometrics

[۲۹] Microchip

قابلیت استفاده چند باره را داشتند. ولی برای ردیابی کالا در زنجیره تولیدی گسترده، جایی که لیبل‌های RFID روی جعبه‌ها و پالت‌های محصولات یک شرکت توسط یک شرکت دیگر قرار داده می‌شود، هزینه بالای آن دیگر توجیه‌پذیر نیست.

از سوی دیگر لیبل‌ها باید در این وضعیت یکبار مصرف باشند. شرکتی که آن‌ها را روی کالا می‌گذارد قادر نیست آن‌ها را مجدداً بازیافت کرده و استفاده کند. آن‌ها همراه با جعبه دور ریخته می‌شوند. از لیبل‌هایی که روی پالت‌ها گذاشته می‌شوند مجدداً می‌توان استفاده کرد و برخی از شرکت‌ها در حال توسعه و ابداع راه‌هایی هستند که بتوان لیبل‌های RFID روی کارتن‌ها را بازیافت کرد.

مرکز تکنولوژی شناسایی اتوماتیک در سال ۱۹۹۹ هیأت ارائه کد استاندارد یا UCC[۳۰] و سازمان بین‌المللی کد گزاری EAN[۳۱] که منشأ آن اروپایی است با مشارکت دو غول بزرگ آمریکایی یعنی شرکت Gillette و Procter Gamble مرکز تکنولوژی شناسایی اتوماتیک Auto ID Center را در دانشگاه MIT[۳۲] برپاکردند. هدف از تشکیل این مرکز طراحی و روش تولید لیبل RFID به‌طور انبوه و ارزان قیمت (پنج سنت برای هر لیبل) بود.

روش جدید شرکت‌ها را قادر می‌ساخت لیبل‌های RFID را روی هر چه که در اختیار دارند قرار داده و آن را از طریق یک شبکه ایمن و نفوذناپذیر به اینترنت متصل کنند. این مرکز به تدریج از پشتیبانی وزارت دفاع آمریکا و صدها شرکت جهانی از جمله، کیمبرلی کلارک، مترو، تارگت، تسکو، یونیلور و وال مارت برخوردار شد. برای این شرکت‌ها RFID پدیده‌ای جذاب بود زیرا می‌توانستند از طریق آن کالای خود را در کل زنجیره تولید تا ارسال به دست مصرف‌کننده نهایی ردیابی کرده و محل دقیق آن را در طول زنجیره شناسایی کنند.

البته برای خرید لیبل ۵ سنتی هنوز باید چندین سال صبر کرد. لیبل‌های RFID امروزی‌براساس مشخصات و ویژگی‌های بسته‌بندی بین ۲۰ تا ۴۰ سنت قیمت دارند. مرکز Auto ID فعالیت خود را به تولید لیبل ارزان قیمت محدود نکرد. این مرکز کد الکترونیکی کالا یا EPC[۳۳] را ابداع کرد. با استفاده از این روش شماره‌گذاری می‌توان یک شماره سریال منحصر به فرد روی هر کالا و محصول قرار داد.

---

[۳۰] Uniform Code Council

[۳۱] European Article Numbering

[۳۲] Massachusetts Institute of Technology

[۳۳] Electronic Product Code

این سیستم راهی برای ایجاد ارتباط بین لیبل‌ها و دستگاه‌های کدخوان که به آن پروتکل اینترفیس هوایی[۳۴] می‌گویند ارایه داد و شبکه‌ای را طراحی کرد که از طریق آن می‌توان اطلاعات را در یک بانک اطلاعات اینترنتی مطمئن و غیرقابل نفوذ ذخیره کرد . با استفاده از این شبکه می‌توان به میزان نامحدود، اطلاعات مربوط به شماره سریال لیبل را به صورت Online ذخیره کرد و هر کسی که مجوز دسترسی به این اطلاعات را داشته باشد می‌تواند از هر نقطه‌ای در جهان از این اطلاعات استفاده کند.

مرکز Auto ID تکنولوژی خود را به یک سازمان غیرانتفاعی به نام EPC global[۳۵] واگذار کرد. این سازمان به سهم خود نسل دوم پروتکل اینترفیس هوایی را ارایه کرد و در حال حاضر سرگرم توسعه ساختار شبکه‌ای به نام EPC global Network است تا از طریق آن شرکت‌ها بتوانند به‌طور همزمان و لحظه‌ای تبادل اطلاعات کنند. نحوه عملکرد شبکه به گونه‌ای است که وقتی شرکت A یک پالت مملو از نوشابه ارسال می‌کند، لیبل‌های روی جعبه‌ها و پالت در حالی که محموله از انبار خارج می‌شوند اسکن می‌شوند و سپس نرم‌افزار به‌طور خودکار به شرکت B اطلاع می‌دهد که محموله از انبار خارج شده است. شرکت B می‌تواند به اطلاعات مربوط به شماره سریال کالا مراجعه کرده و از نوع کالایی که ارسال شده و زمان رسیدن آن به مقصد و اطلاعات دیگر آگاهی پیدا کند. هنگامی که شرکت B محموله را دریافت می‌کند به‌طور خودکار لیبل‌ها را اسکن می‌کند و یک پیام به‌طور خودکار به شرکت A ارسال شده و شرکت را از رسیدن محموله به مقصد آگاه می‌کند. کارآیی این سیستم و شفافیتی که در کارها به وجود می‌آورد فوق‌العاده است. با استفاده از این سیستم شرکت‌ها می‌توانند موجودی انبار خود را همواره کنترل کرده و کاهش دهند و در عین حال مطمئن شوند کالا در زمان مناسب در مکان مناسب است و از آن‌جا که هیچ نیروی انسانی نباید لیبل‌ها را اسکن کند هزینه نیرو و خطای انسانی کاهش فراوان می‌کند. هدف و بینش نهایی این است که زنجیره تولید جهت عکس پیدا کند. امروزه شرکت‌ها براساس پیش‌بینی‌های ماهانه خود کالا تولید می‌کند .سپس آن‌ها کالای تولید شده را به بازار وارد کرده (Push) و به امید فروش همه آن‌ها منتظر می‌مانند.

اگر تقاضا بیشتر از پیش‌بینی‌ها باشد آن‌ها پول از دست می‌دهند. اگر کم‌تر از پیش‌بینی باشد مازاد تقاضا پایین‌تر از قیمت واقعی به‌فروش رفته و یا دور ریخته می‌شود. اگر شرکت‌ها می‌توانستند کالا را براساس تقاضای موجود بازار تولید کنند (Pull) آنگاه نه‌تنها بیشتر سود می‌کردند بلکه ساختار کارآمدتری نیز پیدا می‌کردند .

---

[۳۴] The Air Interface Protocol

[۳۵] Electronic Product Code

کدخوان‌های RFID که روی قفسه فروشگاه‌ها نصب شده‌اند می‌توانند تعداد محصولاتی را که به‌فروش می‌رسند کنترل و نظارت کنند.

هنگامی که تعداد اجناس روی قفسه کاهش پیدا می‌کند سیستم به‌طور خودکار به مسؤولان انبار هشدار داده و آن‌ها اجناس جدید را دوباره به فروشگاه ارسال می‌کنند. هنگامی که میزان اجناس در انبار کاهش پیدا می‌کند سیستم به سازندگان اطلاع می‌دهد تا کالا ارسال کنند و زنجیره ادامه پیدا کرده و تا تولیدکنندگان مواد اولیه امتداد پیدا می‌کند.

هنوز معلوم نیست چنین بینش اتوپویایی هرگز کاملاً به واقعیت بپیوندد. مهم‌ترین مانع هزینه لیبل‌هاست. مرکز Auto ID پس از پژوهش‌های فراوان به این نتیجه رسید که قیمت لیبل‌ها را هنگامی که ۳۰ میلیارد لیبل به‌طور روزانه مصرف می‌شود می‌توان تا ۵ سنت برای هر لیبل کاهش داد. ولی تا زمانی که لیبل‌ها ۲۵ سنت قیمت دارند هرگز مصرف آن‌ها به ۳۰ میلیارد عدد نخواهد رسید. به همین خاطر در حال حاضر صنعت با مشکلی از جنس مرغ اول آمده یا تخم‌مرغ روبه‌رو است. لیبل‌ها ارزان نخواهند شد مگر این‌که همه از آن استفاده کنند، ولی خیلی‌ها تا زمانی که ارزان نشده از آن استفاده نخواهند کرد.

وال مارت [۳۶]اولین فروشگاه زنجیره‌ای است که تولیدکنندگان کالا را ملزم کرد تا از لیبل‌های RFID روی جعبه‌ها و پالت‌های اجناس استفاده کنند. در ژوئن ۲۰۰۳ این شرکت از ۱۰۰ شرکت بزرگی که تولیدات خود را از طریق این فروشگاه‌ها می‌فروشند درخواست کرد که تا سال ۲۰۰۵ از لیبل‌های RFID روی محموله‌های خود استفاده کنند .یکی از دلایل انتخاب این استراتژی حل مشکل مرغ و تخم‌مرغ بود. اگر تولیدکنندگان بزرگ شروع به خرید لیبل‌ها بکنند قیمت لیبل‌ها کاهش می‌یابد .کاهش قیمت‌ها شرکت‌های کوچک‌تر را نیز ترغیب می‌کند تا از این تکنولوژی استفاده کنند. از این طریق حجم تولید افزایش یافته و قیمت‌ها کاهش بیشتری پیدا می‌کنند.

استراتژی وال مارت برای استفاده از RFID در زنجیره تولید دلیل عمده‌ای است بر این‌که این تکنولوژی پرطرفدار است. ولی این تنها دلیل نیست. عوامل مهم دیگری نیز وجود دارند. یکی از عوامل پیشرفت فوق‌العاده در تولید سیستم‌های RFID با فرکانس‌های مافوق بالاست ؛سیستم‌های UHF قادرند توانایی اسکن دستگاه‌های کدخوان را افزایش دهند .به همین خاطر هنگامی که پالت‌ها از در انبار بیرون می‌روند و یا روی قفسه‌ها در ارتفاع بسیار بالا قرار می‌گیرند. کدخوان‌ها می‌توانند اطلاعات را بخوانند. عامل دیگر تلاش مرکز Auto ID برای طراحی و ارایه سیستمی ارزان‌قیمت بود که براساس استانداردهای فراگیر و انعطاف‌پذیر عمل می‌کند. این یکی از پیش‌نیازهای

---

[۳۶] Wal Mart

عمده برای استفاده از RFID در یک زنجیره تولید و عرضه باز و فراگیر است. به گونه‌ای که یک کمپانی لیبل را روی محصول می‌گذارد و شرکت دیگر در طول زنجیره، اطلاعات روی لیبل را می‌خواند.

فراگیری و گستردگی اینترنت عامل مهم دیگری در شکوفایی تکنولوژی RFID است. البته این عاملی است که بسیاری آن را نادیده می‌گیرند. مرکز Auto ID متوجه شد که از اینترنت می‌توان برای تبادل و تقسیم اطلاعات مربوط به محل کالا در هر نقطه زنجیره تولید و تقاضا استفاده کرد. قبل از این‌که Auto ID ، ایجاد شبکه EPCglobal را پیشنهاد کند هیچ راهی (به جز استفاده از تلفن، فاکس یا ای‌میل) وجود نداشت تا به عنوان مثال شرکت A بتواند شرکت B را از ارسال محموله آگاه کند و شرکت B نیز بتواند به شرکت A اطلاع دهد که محموله رسیده است. با استفاده از شبکه، شرکت‌ها نه‌تنها می‌توانند محل کالا را در طول زنجیره تولیدی شناسایی کنند بلکه آن‌ها می‌توانند اطلاعات مربوط به محل کالا را نیز با یکدیگر مبادله کنند.

نقش تکنولوژی RFID در گذر از بانکداری سنتی به بانکداری الکترونیکی

با توجه به فرایند رشد فناوری اطلاعات و ارتباطات در جهان و توسعه این فناوری در نظامهای اداری و بانکی و همچنن تبدیل شدن فضاهای فیزیکی به محیطهای مجازی، برنامه ریزی برای گسترش کاربرد بانکداری الکترونیکی در کشور گریز ناپذیر است. از سوی دیگر تمایل و اصرار مشتریان به استفاده از روشهای سنتی به دلیل غیر ملموس بودن بسیاری از خدمات سیستم بانکداری الکترونیکی در فضاهای مجازی سبب شده است که روند کاربردی شدن این روش نوین بانکی در جامعه با وجود فراهم بودن زیرساختهای اولیه و تلاشهای فراوان و ارزنده مسئولان نظام بانکی کشور با کندی صورت پذیرد. از این رو به راهکارهایی نیاز است تا تمایل عمومی جامعه و اطمینان خاطر افراد را از روشهای الکترونیکی تأمین نماید. استفاده از شیوه بانکداری دوگانه با استفاده از تکنولوژیهای نوین به توسعه کاربرد بانکداری الکترونیکی در جامعه می انجامد. زیرا این روش امکانات الکترونیکی را در محیط بانک به مشتری معرفی نموده و در صورت تسریع و بهبود در ارائه خدمات اطمینان آنها را در به کارگیری بانکداری الکترونیکی فراهم می سازد. تکنولوژی RFID ، سیستمی را برای عملیات بانکی در روش بانکداری دوگانه پیشنهاد می نماید که با استفاده از آن اتوماسیون پشت باجه و مقابل باجه با هماهنگی و سرعت بیشتر انجام می گیرد و همچنین با فراهم نمودن مدیریت متمرکز بر فعالیت بانکی موجب بهینه شدن عملیات بانکها و در نهایت جلب رضایت مشتریان می گردد. اما تسریع در سرویس دهی و رضایتمندی مشتری در این روش از اهمیت ویژه ای برخوردار است زیرا در صورت عدم رضایت مشتریان، پذیرش اصل الکترونیکی شدن بانکها با چالش جدیدتری مواجه خواهد بود. بنابراین در این راستا باید از تکنولوژی‌های جدید با کاربرد آسان استفاده شود. تکنولوژی شناسایی توسط امواج رادیویی (RFID) یکی از پیشرفتهای علمی و فنی جهان است که می تواند در این راستا مؤثر واقع شود. RFID این قابلیت را دارد که با استفاده از زیرساخت‌های الکترونیکی موجود و بدون ایجاد مزاحمت برای مشتریان، بسیاری از امور بانکی را تسریع دهد و امنیت، دقت و یکپارچگی را برای نظام بانکی کشور به ارمغان آورده و موجبات جلب رضایت خاطر مشتریان را فراهم سازد.

کاربرد RFID در بانکداری الکترونیکی

نقش مؤثر فناوری اطلاعات در توسعه بانکداری بسیار روشن و انکارناپذیر است. تکنولوژیRFID نیز در سالهای اخیر موجب تسریع رشد کاربرد فناوری اطلاعات در سیستم‌های اداری و بانکی گردیده است. در یک سیستم اداری هوشمند سیستم RFID برای ردیابی و مدیریت مدارک استفاده می‌شود. به این صورت که با نصب یک برچسب RFID بر روی اسناد امکان رهگیری و انجام عملیات اداری با دقت ومدیریت بهتری انجام خواهد شد. این تکنولوژی در سال ۲۰۰۵ در بانکداری مورد توجه قرار گرفت.تکنولوژی RFID در بانکداری الکترونیکی موجب تسریع در عملیات بانکی و همچنین تضمین امنیت در مبادلات اوراق بهادار و اسناد می گردد.

کاربرد RFID در اسناد بانکی

استفاده از RFID در اسناد بانکی و اوراق بهادار در دو مرحله اتوماسیون پشت باجه و اتوماسیون مقابل باجه کاربرد خواهد داشت. در واقع در بانکداری دوگانه [۳۷]با استفاده از این تکنولوژی می توان ضمن تأمین امنیت بیشتر، سرعت عملیات بانکی را افزایش داد و از میزان ازدحام در شعب کاست.چک‌های متداول سیستم بانکی، دفترچه‌های حساب‌های مشتریان(پس انداز، قرض الحسنه و ...)، چک‌های رمز دار بین بانکی، چک‌های تضمین شده و اوراق سهام از مواردی هستند که استفاده از RFID در آنها بسیار سودمند می‌باشد.

[۳۷] الکترونیکی و سنتی

RFID در اتوماسیون مقابل و پشت باجه

رضایتمندی مشتری یکی از اهداف اصلی بانک‌ها می‌باشد که برای دستیابی به این مهم همواره برنامه‌ریزی‌ها و تلاش‌های فراوانی در جریان بوده است. کاهش ازدحام مقابل باجه‌ها و تسریع در سرویس‌دهی از عواملی است که موجب جلب رضایت مشتریان می‌گردد. برای سرعت بخشیدن به عملیات بانکی می توان از سیستم RFID استفاده نمود. برای این منظور باید برچسب‌های RFID بر روی اسنادی مانند چک‌ها و دفترچه (کارتهای) حساب مشتری قرار گرفته باشد.

جهت بهبود فرایند در شعب به دو نوع قرائتگرنیاز است:

الف- قرائتگر باجه

این قرائتگر هنگام دریافت سند از مشتری توسط کاربر بانک، به طور خودکار و با استفاده از امواج رادیویی اطلاعات سند را دریافت نموده و با ارتباط با رایانه، بلافاصله مشخصات صاحب حساب یا سند دریافتی را روی صفحه نمایش نشان می دهد. این عمل دو مزیت را در پی خواهد داشت:

۱- صحت سند موردنظر تأیید می شود. به این صورت احتمال جعل و تقلب تا حد قابل ملاحظه‌ای کاهش می‌یابد.

۲- به انجام عملیات دستی و درج مشخصات یا شماره حساب نیازی نیست و این امر موجب تسریع در عملیات خواهد شد.

ب- قرائتگر ویژه مشتریان

این قرائتگر که در بیرون از باجه و در محل حضور مشتریان درون شعبه نصب می گردد می تواند نقش قابل ملاحظه‌ای در کاهش ازدحام پشت باجه‌ها داشته باشد. این قرائتگر با دریافت امواج از برچسب موجود روی سند می تواند اطلاعات مورد نیاز مشتری را نمایش دهد. برای مثال هر گاه روی دسته چک مشتری یا دفترچه حساب برچسب RFID نصب شده باشد، مشتری به این طریق قادر است از موجودی حساب یا گردش حساب خود با استفاده از قرائتگر آگاهی یابد یا سایر اطلاعاتی که ممکن است در مراحل بعدی برای سیستم تعریف شود، به راحتی قابل دسترس می‌گردد. همچنین مشتریان می توانند با استفاده از سیستم RFID از صحت چک‌هایی که در دست دارند، اطمینان حاصل یابند. این روش به خصوص برای تأیید چک‌های مسافرتی و چک‌پول‌ها و شناسایی

موارد جعلی یا سرقت شده برای مشتریان بسیار سودمند است. از سوی دیگر استفاده از تکنولوژی RFID در پشت باجه و برای مدیریت عملیات بانکی مزایای زیادی را به همراه خواهد داشت. ردیابی اسناد، جست و جوی سریع، افزایش امنیت و مدیریت متمرکز از جمله دستاوردهایRFID در اتوماسیون پشت باجه است. همچنین با استفاده از این سیستم به خصوص در شعب بزرگ می توان با توجه به مجهز بودن دفترچه‌ها و دسته چک‌های مشتریان دائمی و اصلی بانک به برچسب RFID در بدو ورود آنها را شناسایی نموده و از مشتریان غیر ثابت تفکیک کرده و برای جلب رضایت آنها سرویس‌هایی را ارائه نمود. از سوی دیگر تکنولوژی RFID توانایی استفاده در تلفن‌های همراه را نیز دارد و به این ترتیب در آینده نقش بزرگی در بانکداری مبتنی بر تلفن همراه ایفا خواهد نمود.

بانکداری الکترونیکی در کشور ما از سابقه زیادی برخوردار نیست. هرچند در مدت زمان کوتاهی نظام بانکی ایران موفق شده است در روشهای بانکداری الکترونیکی و اینترنت بانک به دستاوردهای ارزنده ای دست یابد اما باید پذیرفت عوامل زیادی در این راستا دخیل هستند تا این شیوه‌ی نوین بانکی را در جامعه نهادینه نمایند. بدیهی است مشتریانی که سالها از خدمات بانکداری سنتی استفاده کرده اند به یکباره به سوی شیوه های جدید روی نخواهند آورد. در سالیان متمادی سعی شده است اعتبار بانکها در داشتن مکان‌های فیزیکی و ساختمان‌های مجهز و متعدد به مشتریان القا شود. کارکنان بانک‌ها روشهای ارتباط مناسب با مشتریان را آموزش می‌بینند و مدیریت ارتباط با مشتری به عنوان یک رکن اصلی در دستور کار برنامه‌ریزان بانک‌ها قرار می گیرد. مشتریان نیز به نوعی حضور فیزیکی را در بانک موجب اطمینان خاطر از صحت انجام مبادلات خود تلقی می‌کنند و اعتباری را که در یک رسید کاغذی در ذهن خود ایجاد نموده اند به راحتی با روشهای دیگر معاوضه نخواهند کرد. واضح است که برای رسیدن به نظام بانکی الکترونیکی به غیر از فراهم نمودن بسترهای تکنولوژی و فنی با موارد دیگر نیز مواجه هستیم. از این رو برای گذر از بانکداری سنتی به سمت بانکداری الکترونیکی باید با راهکارهای مؤثری مورد استفاده قرار گیرند. توجه به بانکداری دوگانه یکی از این راهکارها است که در تمام مراحل کاربرد خواهد داشت. به این طریق فرهنگ لازم جهت پذیرش شیوه‌های نوین به ندرت در جامعه پرورش می‌یابد. اما شاید به اعتقاد عده ای بانکداری دوگانه بسیاری از نیازهای بانکی امروز را مرتفع ننماید.

در این راستا تکنولوژی‌های جدید به عنوان ابزاری ارزشمند در خدمت پیشرفت امور بانکی قرار گرفته‌اند. تکنولوژی شناسایی از طریق امواج رادیویی یکی از روش‌هایی است که در سالهای اخیر به شدت مورد توجه سیستم‌های اداری و صنایع در کشورهای مختف قرار گرفته است.RFID این قابلیت را دارد که در شرایط کنونی

و در کنار روش‌های نوین بانکی مانند اینترنت بانک یا بانکداری متنی بر تلفن همراه، بسیاری از نیازهای شبکه بانکی و مشتریان را تأمین نماید. استفاده آسان، امنیت بالا ،تسریع در انجام امور و توانایی ارتباط با شبکه‌های رایانه‌ای و امکان یکپارچه سازی عملیات بانک‌ها از مهمترین مواردی است که استفاده از RFID را از هر لحاظ سودمند نموده است.RFID جانشین مناسبی برای کارت‌های مغناطیسی برای فعالیت تجاری خارج از محیط بانک و راهکاری ارزشمند برای عملیات درون بانک با تکیه بر ابزار الکترونیکی خواهد بود. بکارگیری این تکنولوژی در این مقطع زمانی با شرایط فرهنگی جامعه مطابق بوده و با توجه به سرویس دهی مناسب، ایمن و سریع راه را برای توسعه بانکداری الکترونیکی هموار می سازد و ضمن روان سازی عملیات درون شعب به رضایتمندی مشتریان نیز کمک قابل توجهی می‌نماید.

کنترل بیومتریک

واژه بیومتریک [۳۸] از کلمه یونانی بیوز [۳۹] به معنای زندگی و متریکوز [۴۰] به معنای اندازه گیری تشکیل شده است .
امروزه در زمینه های فراوانی ما به وسایلی نیاز داریم که هویت اشخاص را شناسایی کند.
بر اساس ویژگی های بدن اشخاص آنها را باز شناسی کند و بیومتریک علمی است که به شناسایی مشخصه های طبیعی و رفتاری هر انسان برای تعیین یا تصدیق هویت وی می پردازد.

فناوری بیومتریک به عنوان یکی از فناوری سامانه بیومتریکی، یک سامانه تشخیص الگو است که هویت اشخاص را تعیین یا تأیید می کند و این عملیات را با استفاده از اطلاعات بیومتریک کاربران انجام می دهد.
نخستین گام در استفاده از این سامانه ثبت اطلاعات بیومتریکی کاربران در بانک اطلاعات سامانه است که پس از ثبت اطلاعات افراد در این سامانه، دو نوع خدمت از سامانه بیومتریکی درخواست می شود.

---

[۳۸] Biometric

[۳۹] BIOS

[۴۰] METRIKOS

تأیید هویت و تعیین هویت

آزمایش زیست سنجی دانش مدیریت بانکی[۴۱] در سامانه بیومتریک شامل سه گام است : ثبت مشخصات ، مقایسه و به روزرسانی.

تعیین یا تأیید هویت افراد هنگام انجام تراکنش های مالی، کاربرد بیومتریک ها در این عرصه را رقم می زند . این کاربرد که در سال های اخیر توسعه یافته است جهت تکمیل یا جایگزینی فرایند ورود به سامانه های مالی الکترونیکی به روشی آسانتر و البته مطمئن تر مورد استفاده قرار م یگیرد.

بانک ها و مؤسسات مالی بزرگی در سراسر جهان به استفاده از سامانه های بیومتریکی در این حوزه روی آورده اند .طیف وسیعی از بیومتریک ها در این حوزه مورد استفاده قرار میگیرند که از آن جمله عبارتند: انگشت نگاری، عنبیه نگاری، چهره نگاری و اسکن الگوی رگ های دست.

فناوری بیومتریکی دربخش بانکداری و خدمات مالی رشد چشمگیری داشته است .این فناوری نه تنها امنیت و ارائه خدمات را افزایش می دهد بلکه امکانات ارزشمند جدیدی از جمله خدمات از راه دور را به ارمغان آورده است.نهایی شدن استانداردهای فرمت داده های بیومتریکی و رمزگشایی آنها شامل , BAPI[۴۳] , BioAPI [۴۲] CBEFF[۴۴] و X9.84 باعث پذیرش بیشتر آن در صنعت شده است.

البته به علت محافظه کاری بسیاری از مؤسسات و ترس از رخنه افراد سودجو، امکانات بالقوه بسیاری برای توسعه وجود دارد که هنوز توسعه نیافته اند.

از اوایل سال ۲۰۰۱ استفاده از فناوری های مختلف بیومتریکی کاربردهای موفقیت آمیزی در این بخش داشته اند . لذا به دلیل اهمیت این فناوری در حوزه بانکداری الکترونیک گزارش حاضر به شرح این فناوری و کاربرد آن در بانک می پردازد.

---

[۴۱] Knowledge Of Banking Management

[۴۲] Biometric Application Programming Interface

[۴۳] Business Application Programming Interface

[۴۴] Common Biometric Exchange Formats Framework

بیومتریک های فیزیولوژیکی

- **انگشت نگاری**

کاربر خیلی آرام انگشت خود را روی سطح سنسور بیومتریک سیلیکونی یا نوری با ابعاد یک تمبر پستی قرار می دهد. مدت زمان استاندارد برای تصدیق هویت از زمان اعلان سیستم، دو تا سه ثانیه است.

- **چهره نگاری**

کاربر با فاصله ترجیحاً شصت سانتی متری مقابل یک دوربین قرار می گیرد .مدت زمان استاندارد برای تصدیق هویت از زمان اعلان سیستم سه تا چهار ثانیه است.

- **عنبیه نگاری**

کاربر در مقابل نرم افزار خاصی نظیر دوربین ویدیویی قرار می گیرد .طوری چشمان خود را روی دستگاه متمرکز میکند که قادر به مشاهده تصویر چشمان خود باشد.مدت زمان استاندارد برای تصدیق هویت از زمان اعلان سه تا پنج ثانیه است.

- **شبکیه نگاری**

کاربر به یک دریچه کوچک بر روی میز یا دیوار نگاه می کند.چشمان خود را درحالیکه به یک شعاع نور سبز کوچک در داخل دستگاه خیره شده است ثابت نگه می دارد . مدت زمان استاندارد برای تصدیق هویت ده تا دوازده ثانیه است.

- **روش های استفاده از دست جهت تایید هویت**

انواع این روش ها عبارتند از:

هندسه دست، هندسه انگشتان، عروق دست، خطوط کف دست و اثر انگشتان.

انواع بیومتریک های رفتاری

- **صوت نگاری**

کاربر درمجاورت یک دستگاه ضبط صدا نظیر میکروفن یا تلفن قرار میگیرد .با اعلان سیستم کاربر عبارت عبور ثبت شده را می گوید .زمان استاندارد برای تصدیق هویت چهار تا شش ثانیه است.

- **اسکن امضا**

فرایند نشانه گذاری سریع (از قبیل سرعت، فشار، خط سیر قلم و...) برای هر شخص منحصر به فرد است .برای ثبت امضا از یک اسکنر مخصوص استفاده می شود .این اسکنر نه تنها شکل امضا را اسکن می کند بلکه طرز امضا کردن را هم می سنجد .به این مفهوم که مناطقی را که قلم را فشار دادید یا تند حرکت دادید و یا برعکس مناطقی از امضا را که خط نازک کشیدید، ثبت و مقایسه میکند و به این ترتیب جعل امضا غیر ممکن می شود . با اعلان سیستم کاربر تنها نام خود را بر روی تخته مخصوص امضا می کند .مدت زمان استاندارد چهار تا شش ثانیه است.

- **اسکن تایپ**

اسکن تایپ کاربر، تنها به مدت زمان استاندارد دو تا سه ثانیه است .نام کاربری وکلمه عبور خود را تایپ می کند.

مهمترین کاربرد های بیومتریک در صنعت بانکداری الکترونیکی

- **دسترسی به حساب ها**

یک مثال خوب در این زمینه" وسترن بانک[۴۵] "پورتوریکو است که از اواسط سال ۲۰۰۰ ، تمامی ۳۷ شعبه خود را به سامانه تشخیصی اثر انگشت و اسکن امضا مجهز کرد .آمارها نشان می دهد در همان ابتدا۱۰تا ۱۵درصد از۳۰۰ هزار مشتری بانک از سامانه بیومتریکی استفاده کردند.

هزینه تقریبی راه اندازی این سامانه ۳ میلیون دلار برآورد شد .بزرگترین بانک بخش خصوصی برزیل هم از فناوری صوت نگاری برای اجازه دسترسی تلفنی مشتریان خود به حساب هایشان استفاده کرده است.

- **خودپردازها**

برای بعضی تراکنش ها، بیومتریک ها می توانند یک گزینه مناسب در خودپردازها باشند.

درسال۱۹۹۷ یک موسسه مالی و اعتباری در سوئد و انگلیس طرح آزمایشی بر پایه سامانه عنبیه نگاری در خودپردازهایش را به اجرا گذاشت . نتیجه موفقیت آمیز این طرح استفاده بیش از ۹۴ درصد از مشتریان و ترجیح این فناوری نسبت به سامانه PIN[۴۶] بود . پروژه های مشابهی در امریکا، هند، آلمان و ...اجرا شده که با استقبال فراوانی مواجه شده اند.

بانک های بزرگ جهان از جمله امپریال کانادا با استفاده از فناوری عنبیه نگاری و میتسوبیشی ژاپن با استفاده از فناوری رگ نگاری کف دست از پیشتازان استفاده از خودپردازهای بیومتریکی در دنیا می باشند .بانکداری الکترونیک و بلادرنگ، تراکنش های تلفنی، دسترسی به PC[۴۷] و شبکه های کامپیوتری و دسترسی فیزیکی به منابع از موارد دیگر در این زمینه هستند که در امریکا، آلمان، کانادا، مالزی و ... بیشترین استفاده مشاهده شده

---

[۴۵] Western Bank

[۴۶] Personal Identification Number

[۴۷] Personal Computer

است .با توجه به پروژه های بزرگی که هم اکنون در بخش بانکداری کشور در حال اجراست(از جمله پروژه شتاب) توجه ویژه به قابلیت های بیومتریکی می تواند حایز اهمیت باشد.

- **تجارت الکترونیک / تلفنی**

کاربردهای این حوزه بیشتر مربوط به تراکنش های از راه دور (خصوصاً تلفنی یا اینترنتی) می باشد.
در اینجا هم بیومتریک ها به منظور تکمیل یا جایگزینی فرایند ورود به سامانه مورد استفاده قرار میگیرند .یکی از مهمترین مزایای استفاده از سامانه بیومتریکی در این فرایندها عدم نیاز به سرپرست یا ناظر ورود و تصدیق هویت افراد می باشد.
صوت نگاری از جمله بیومتریک ها پرکاربرد در این حوزه می باشد.

بانک ملت و فناوری بیومتریک

سیستم بیومتریک در تمامی شعب بانک ملت وجود دارد.در این سیستم، احراز هویت و شناسایی مشتریان بانک از طریق اثر انگشت انجام می شود.این فناوری با هدف کاهش هزینه های عملیاتی و افزایش سرعت ارایه خدمات، همچنین افزایش کنترل های داخلی بدون ایجاد تاخیر در فرآیند ارایه خدمات بانکی، مورد استفاده قرار گرفته است . این فناوری در مرحله اول در مورد حساب های قرض الحسنه و کوتاه مدت قابل استفاده بود . در حساب های جاری علاوه بر احراز هویت به سبک سنتی از طریق تطبیق چهره مشتری با مدارک ارایه شده از سوی وی کنترل های مضاعفی هم مثل سریال برگ چک وجود دارد که امکان سوءاستفاده را کاهش می دهد . ولی در حساب های قرض الحسنه و کوتاه مدت ، این ویژگی دسته چک وجود ندارد .هدف سیستم بیومتریک، انجام کنترل های مضاعف در جهت احراز هویت صاحب حساب به هنگام مراجعه به شعب است ، مشتریان بانک ملت هر زمان که علاقه مند باشند می توانند با مراجعه به شعب و ثبت اثر انگشت خود روی پایگاه داده های بانک ، از امکان تطبیق اثر انگشت خود به هنگام انجام عملیات بانکی برخوردار شوند .در این صورت حتی اگر مشتری، مدارک احراز هویت را به همراه نداشته باشد ، بانک می تواند در زمانی کوتاه، بدون هیچ گونه دغدغه ای با تطبیق اثر انگشت ، خدمات مورد نیاز را به وی ارایه دهد .بیش ا ز ده هزار مشتری این بانک متقاضی استفاده از این سیستم در کمتر از یک ماه بودند . همه مشتریان بانک می توانند از این مزیت بهره مند شوند ، چون متناسب با حجم و تعداد مشتریان شعب، سخت افزار خریداری و در شعب بانک از یک تا چهار دستگاه اسکنر اثر انگشت نصب شده است .سیستم بیومتریک هم اکنون درتمام شعبه بانک در استان تهران و اکثر شعبه در استان های سراسرکشور عملیاتی شده است .این فناوری قابلیت تسری به دستگاه های خودپرداز و پایانه های فروشگاهی جدید را نیز دارد.

بازکردن حساب، درخواست وام و یا مسدود کردن کارت اعتباری بدون اینکه نیاز به مداخله کارمند انسان باشد استفاده کنند.

نقش بانکها در مشخص کردن هویت فرستنده در نقل و انتقال الکترونیکی

بانک‌ها در نقل و انتقال الکترونیکی هویت کامل فرستنده را مشخص کنند ؛ بانک مرکزی اعلام کرد ، بانک‌ها و موسسات مالی باید در روابط کارگزاری خود ، به ویژه درنقل و انتقالات الکترونیکی برون مرزی با سایر موسسات هویت کامل فرستنده و ذینفع وجه و نیز ماهیت کسب و کار و هدف آنها از این نقل و انتقال را مشخص کنند.

به گزارش گروه بانک و سرمایه گذاری پول نیوز ، بانک مرکزی آمده است: اطلاعات فرآیند نقل وانتقال الکترونیکی برون مرزی وجوه، باید به صورت استاندارد در فرمت‌های سوئیفت درج شده و در تمامی مراحل نقل و انتقال، همراه پیام باشد.

این گزارش می‌افزاید: شناسایی کافی هویت فرستنده و ذینفع وجوه در پرداخت‌های الکترونیکی در زمره مقولاتی جای می‌گیرد که درمبادلات برون‌مرزی از اهمیت فراوانی برخوردار بوده و در استانداردهای بین‌المللی ناظر برمبارزه با پولشویی و تامین مالی تروریسم نیز بر آن تاکید زیادی شده است.

در ادامه آمده است:نظر به اهمیت موضوع، کمیته نظارت بانکی بال به عنوان یکی از مراجع پیشرو در زمینه گسترش مفاهیم نظارت بانکی، در سال ۲۰۰۹ میلادی اقدام به انتشار سند مهمی در این زمینه با عنوان'شناسایی کافی و شفافیت در پیام‌های پرداخت پوششی در نقل و انتقالات برون مرزی وجوه' نمود.

این سند مشتمل بر ارایه تعاریف هریک از مفاهیم مربوط بوده و به شناخت عمیق تری از این پدیده‌ها می‌انجامد. شناختی که همراه با معرفی مجموعه تدابیری است که در مدیریت موثر روابط کارگزاری با سایر بانک‌ها و نظارت کارآمد بر این روابط (از سوی مراجع نظارت بانکی)، به کار می‌آید.

در ادامه این اطلاعیه آمده است :اهمیت سند مذکور موجب شد تا ترجمه آن در دستور کار اداره مبارزه با پولشویی بانک مرکزی جمهوری اسلامی ایران قرار گیرد تا در کنار سایر اسنادی که تاکنون در این زمینه و توسط این بانک ترجمه و منتشر شده است؛ مرجع مناسبی را برای نظام بانکی و کارشناسان، محققان و دیگر اشخاص علاقه‌مند به مباحث بانکی، نظارتی و مبارزه با پولشویی و تامین مالی تروریسم فراهم آورد .

سامانه استعلام بر خط تایید اصالت مشتریان بانک ملت

بانک ملت به عنوان اولین بانک کشور با همکاری سازمان ثبت احوال کشور ، از سامانه ی استعلام بر خط تایید اصالت مشتریان رونمایی کرد.

در مراسم رونمایی از این سامانه که با حضور رییس سازمان ثبت احوال کشور و معاونان وی ،مدیر عامل و جمعی از مدیران ارشد بانک ملت بر پا شد ، نفاهم نامه ی همکاری با موضوع امکان بهره برداری از سامانه ی استعلام الکترونیک هویت ملی به صورت بر خط ،به امضای طرفین رسید.

سامانه استعلام تایید اصالت مشتریان با هدف احراز هویت مشتریان ، به حداقل رساندن زمان انتظار مشتری در ارائه سرویس ها و خدمات ،جلوگیری از سو استفاده از مشخصات سجلی افراد و کاهش ریسک ناشی از تاخیر زمانی تایید اصالت توسط متخصصان داخلی طراحی و در بانک ملت پیاده سازی شده است.

با این سامانه تمامی شعب بانک ملت می توانند از خدمات استعلام بر خط هویت افراد بهره مند شوند و بدین ترتیب موارد سو استفاده از اسناد هویتی یه حداقل ممکن کاهش خواهد یافت .

بانک یک سازمان مالی است که به دلیل تبادل پولی حساسیت کار آن بسیار زیاد است و لازم است قبل از ارائه خدمات به مشتریان ،از اصالت و هویت آنان مطلع شود به عبارت دیگر تایید اصالت هویت ملی افراد این اصل مسلم برای هر بانک است.

تایید اصالت مشتریان به دلیل نداشتن دانش و مهارت کشف تقلب از کنترل سیستم های داخلی بانک خارج است.از سال ۸۶ سامانه استعلام آفلاین هویت افراد در بانک ملت راه اندازی شد و زمینه اتصال آنلاین سامانه بانکداری متمرکز بانک ملت به سامانه ثبت احوال فراهم شد و گامی بزرگ در جهت ارتقا سطح این سیستم برداشته شده است.

اینترنت، امنیت و هویت

دزدی هویت از طریق اینترنت بیش از پیش به یک دغدغه تبدیل می شود، و این امنیت افراد را به مخاطره می افکند.شناسایی و تعیین هویت فرآیند معمولی و مهمی است که ما در انجام دادن امور روزمره خویش دایماً با آن مواجه هستیم. شرکت ها، نهادهای دولتی و مؤسسات به طور معمول برای شناسایی و احراز هویت فردی در مقابل فرد دیگر، از افراد می خواهند اطلاعات شخصی خود را به آن سازمان بدهند. در گذشته رسم بر این بود که مردم به تبادل رخ به رخ اطلاعات و تأیید هویت اتکا می کردند، اما امروزه با پیدایش پدیده «اینترنت»، این روش تا حدودی قدیمی شده و از عیار افتاده است. اطلاعاتی که سابقاً در کشوهای کمد و در محل امن نگهداری می شد اکنون در پایگاه داده ها جمع آوری و ذخیره می شود. آیا این سیستم سریع و کارآمد امنیت اطلاعات شخصی ما را از بین می برد؟ آیا واقعاً اطلاعات شخصی و داده های پایه و ابتدایی برای تعیین هویت ما در شبکه اینترنت از امنیت برخوردار است؟

در دنیای مجازی اینترنت، از ابزار تأییدِ هویت چندان خبری نیست، زیرا تأیید هویت فناوری خاصی- نظیر مشخصات بیومتریک- می طلبد که در سطح گسترده و عام استفاده نمی شود. رایج ترین شیوه های تأیید هویت همانا استفاده از رمز عبور [۴۸] ، شماره حساب یا داده های مشابه هویتی است. به طور مثال، افراد صرفاً با درج شماره حساب و رمز عبور می توانند به اطلاعات حساب بانکی دسترسی پیدا کنند. در واقع امکان دسترسی به اطلاعات مورد نیاز برای هر کسی که این اطلاعات کلیدی را داشته باشد مهیاست.

[۴۸] PASSWORD

دزدی هویت

دزدی هویت زمانی رخ می دهد که شخصی اطلاعات پایه و مقدماتی، همچون نام، نشانی و شماره کارت اعتباری یا شماره بیمه تأمین اجتماعی- فرد دیگری را بدست می آورد و از آن برای افتتاح حساب بانکی، سفارش کالا، استقراض یا تصاحب هویت شخصی دیگری استفاده می کند. به عنوان نمونه، آدام مارلین از شبکه خبری س.ان.ان [۴۹] با پزشکی که اخیراً قربانی دزدی هویت شده مصاحبه و مطالب ذیل را آشکار کرده است. «ایگناسیو رامیرز»، ساکن سَن دیه گو (ایالت کالیفرنیا)، می گوید در فوریه سال گذشته شخصی از یک شرکت تولید کننده تجهیزات پزشکی در بوستون با وی تلفنی تماس گرفت و مبلغ هشتاد و پنج هزار دلار را بابت خرید لوازم پزشکی از وی مطالبه کرد. «رامیرز» شخصاً چنین خریداری نکرده بود، ولی چند هفته بعد فهمید که اطلاعات شخصی او را دزدیده اند؛ زنی اطلاعات شخصی «رامیرز» را از طریق اینترنت بدست آورده و به این ترتیب توانسته بود به اطلاعات لازم برای احراز هویت- ازجمله شماره پروانه طبابت و شماره بیمه تأمین اجتماعی- او که آن زمان برای خرید تجهیزات پزشکی استفاده می شد دست پیدا کند. متأسفانه مشابه این وضعیت چندان غریب و نامتعارف نیست و بسیار شایع است. خلاف کاران برای بدست آوردن اطلاعات شخصی مردم از شیوه های متعددی نظیر کیف قاپی، نامه دزدی، زیرنظر گرفتن افراد در مقابل باجه های خودپرداز [۵۰] و زیر و رو کردن و جست وجو در میان زباله ها بهره می گیرند، اما به نظر می رسد اینترنت به روش منتخب آنها بدل شده است.

دزدی هویت از طریق اینترنت بیش از پیش به یک دغدغه تبدیل می شود، زیرا اکنون مردم از انواع مشکلات ناشی از نحوه جمع آوری، نگهداری و نشر همزمان اطلاعات شان در اینترنت آگاهی دارند. نخست این که اینترنت، شرکت ها، مؤسسات و نهادهای دولتی را تشویق می کند که اطلاعات بیشتری را از افراد جمع آوری کنند، زیرا می توان داده ها را به آسانی و به طور کارآمد، ضبط و ذخیره کرد. این سیستم جمع آوری و ذخیره اطلاعات برای شرکت ها و نهادهای دولتی کار کرد بسیار خوبی دارد. ولی امنیت افراد را به مخاطره می افکند، زیرا به متخلفان این عرصه محلی را معرفی می کنند که آنها می توانند به مقادیر معتنابهی از اطلاعات شخصی افراد وسعت پیدا کنند. محض مثال، اگر شخصی به دنبال نام و شماره تلفن یا نشانی و حتی شماره بیمه فردی باشد می تواند از طریق یک منبع عمومی و تقریباً به آسانی به خواسته های خود دسترسی پیدا کند.

---

[۴۹] CNN

[۵۰] ATM

دیگر مشکل نگران کننده به میزان نشر و توزیع اطلاعات شخصی افراد مربوط می شود. دستیابی به اکثر خدمات اینترنتی online ، مستلزم تکمیل کردن فرم هایی است که امکان دسترسی به اطلاعات خواسته شده را برای متقاضی فراهم می کند. معمولاً این فرم شامل اطلاعاتی در فرم هایی از پیش تهیه شده، مشکلات امنیتی به بارمی آورد، زیرا اصولاً مصرف کنندگان به این قبیل اطلاعات هیچ گونه کنترلی ندارند و ضوابط و قوانین فدرال هم وجود ندارد که صاحبان آن نهادها و ارگان های خدماتی در انیترنت را از فروش اطلاعات به خریداران دیگر باز دارد. بنابراین، سرانجام ممکن است اطلاعات مشخص افراد در فهرست مکاتبات چندین و چند مؤسسه و ارگان قرار گیرد و میان تعداد کثیری از شرکت های مختلف توزیع شود. خطر سوءِ استفاده از این قبیل اطلاعات با پخش و درز گسترده آن در جاهای متعدد، افزایش می یابد. دیگر ویژگی مفید اینترنت، امکان متصل شدن به جاهای دیگر است و این ویژگی به سازمان ها امکان می دهد که سوابق و سندهایی از منابع دیگر را برای مقاصد خود استفاده و نگهداری کنند. به طور مثال، بانکی که به درخواست اخذ وام مشتری رسیدگی می کند در عرض چند ثانیه می تواند صورت وضعیت حساب متقاضی و اطلاعات مربوط به آن را بدست آورد. این ویژگی هم مفید و هم در صورت درز کردن نزد متخلفان، بسیار زیان آور خواهد بود، به طوری که آنها با سرعت بیشتر و بدون صرف زمان برای گردآوری اطلاعات مختلف از جاهای مختلف به مجموعه اطلاعات مشخصی یک فرد دست یابند. به عنوان نمونه، اکثر سازمان ها در ایالات متحده برای شناسایی مشتری یا متقاضی و مخاطب خود از شماره بیمه تأمین اجتماعی استفاده می کنند که با درج که مربوط، اطلاعات فراوانی در خصوص سوابق پزشکی، اطلاعات بانکی و سوابق اعتباری مشخص به دست می آید.

سرانجام این که در اینترنت برای تأیید هویت افراد از ابزاری نظیر اثر انگشت یا عکس کاربر استفاده نمی شود و فقط از یک کد کاربری و رمزعبور استفاده می گردد و با درج این قبیل داده ها، هرکس به اطلاعات دست می یابد. یکی از روش های متخلفان اینترنتی برای دستیابی به این دو عامل شناسایی، ارسال نامه های الکترونیکی ناخواسته [۵۱] و وعده کردن اعطای برخی امتیازات و در کنار آن درخواست اعلام اطلاعات ویژه همچون شماره حساب برای بهره مندی از آن امتیازات و منافع مالی وعده داده شده است.

[۵۱] spam

ابعاد جالب اینترنت برای دزدی هویت

اینترنت جایی است که می توان به آسانی و به سرعت و به وسیله یک دستگاه رایانه رومیزی یا رایانه قابل حمل به اطلاعات شخصی مردم دست پیدا کرد.ناشناس بودن در اینترنت هم یکی از ویژگی های جالب و جذاب نزد اکثر متخلفان اینترنتی است. در گذشته، جعل هویت مستلزم ارائه اسناد و مدارک شناسایی به صورت حضوری و رو در رو بود و فقط یک بار امکان انجام دادن آن وجود داشت. اما اینترنت به خلاف کاران امکان می دهد که این کار را چند مرتبه انجام بدهند و در محلی امن، نسبتاً ناشناس بمانند.

نکته آخر این که اینترنت به موقعیت های جغرافیایی متکی نیست. متخلف می تواند اطلاعات مشخص فردی را که به وی ظن نمی برد از آن سوی دنیا دریافت کند.

راه های محافظت در برابر دزدی هویت در اینترنت

بهترین راه حل ممکن برای حفاظت اطلاعات اینترنتی همانا مجهز شدن به فناوری پیشرفته و تدوین ضوابط دقیق از سوی دولت است. پول و امضای الکترنیک مصداق فناوری پیشرفته است. امضای الکترونیک از ابراز رمزنگاری است که اصولاً جایگزین روش های قدیمی و سنتی تعیین هویت شده است. امضای الکترونیک یا همان امضای دیجیتال رمزی است که توسط دارنده آن برای امضا کردن و پیامدهایی که با کلیدهای عمومی تأیید هویت می شوند، استفاده می کند. در پول الکترونیک هم مانند امضای دیجیتال از همان الگوی به رمز درآوردن استفاده می شود و این امکان را می دهد که مشخص دیگری نتواند آن را ردیابی کند و خود پول هم ناشناس بماند. «بیومتریک» هم ازجمله دیگر راه کارهای جلوگیری از دزدی هویت به شمار می آید که در آن برای تعیین هویت فرد از ویژگی های اجزای بدن او استفاده می شود. به عنوان مثال، از اثر انگشت یا شبکیه چشم انسان می توان برای تأیید هویت بهره برد. این روش ها به رغم مفید بودن در جلوگیری از دزدی هویتی، محدودیت هایی نیز دارند که باید مورد توجه قرار بگیرد.

تدوین و اتخاذ ضوابط و معیارهای بین المللی برای کنترل و تأمین امنیت اطلاعات شخصی نیز در مبارزه با دزدی هویت دولت هاست، اما باید این نکته را نیز مطمح نظر قرار داد که در این صورت هم، دولت کماکان به اطلاعات شخصی افراد دسترسی خواهد داشت. البته راه های ساده تر دیگری هم برای جلوگیری یا حداقل کاستن از بروز دزدی هویت وجود دارد، علم و آگاهی به سیاست های حفظ حریم خصوصی افراد در خدمات اینترنتی و قدری خسّت در ارائه اطلاعات در اینترنت هم ازجمله دیگر ابزار محافظت در برابر دزدی هویت به شمار می رود. نمونه آن، پیام های ناخواسته اینترنتی در قالب نامه های الکترونیکی ناآشنا یا ناشناس است که می توان هیچ تربیت اثری به آنها نداد. بنابراین، برای کاربران اینترنتی مهم است که از میزان آسیب پذیری اطلاعات شخصی شان در خدمات اینترنتی آگاهی داشته باشند. این آسیب پذیری، نتیجه عوامل خارجی است از جمله: نحوه اداره و کنترل اطلاعات شخصی افراد توسط شرکت های ارائه کننده خدمات اینترنتی و شناسایی داده ها و ویژگی های خاص اینترنت. شرکت های خدمات اینترنتی اطلاعات شخصی را به گونه ای جمع آوری، نگهداری و توزیع می کنند که زندگی افراد (کاربران) را به کتابچه ای سرگشاده مبدل می کند که هرکس می تواند آن را بخواند. بنابراین، به منظور جلوگیری از دزدی هویت باید به این نکته توجه داشته باشیم که نقش شرکت های ارائه کننده خدمات اینترنتی و خود اینترنت به اندازه نقش دزدان هویت و «هَکِر» ها اهمیت دارد.

چگونگی حفاظت از حسابهای بانکی و اطلاعات هویتی

هویت و اطلاعات شخصی شما به دلایل متعدد بسیار با اهمیت هستند. شما ممکن است زمانی متوجه شوید قربانی یک کلاهبرداری شده اید که نامه ای دریافت نمایید که در آن از شما خواسته شده بدهی های معوقی که متعلق به شما نیست را پرداخت نمایید. در صورتی که هیچ گاه چنین وام یا قرضی از بانک نگرفته اید.

حل این مسائل بسیار زمان بر و خسته کننده است. در ادامه به نکاتی اشاره می شود که با به کارگیری آنها می توان از اطلاعات محرمانه خود بهتر حفاظت کرد.

●از اسناد با ارزش محافظت کنید

مراقبت از اسناد با ارزش مانند گذرنامه، گواهینامه،کارت ملی، کارت های بانکی و دفترچه های حساب بانکی بسیار با اهمیت است. همیشه مطمئن شوید که این اسناد درهرجا چه خانه و چه محل کار و یا هنگامی که در مسافرت هستید در دسترستان هستند. زمانی که از این اسناد استفاده نمی کنید بهتر است آنها را در گاوصندوق در خانه نگه دارید. همیشه به یاد داشته باشید که کارت های بانکی خود را در مکانی جدا از کلمه عبور آنها نگه دارید.

●تمام اسناد اداری زائد را از بین ببرید

به کلاهبرداران فرصت طلب کمک نکنید. همیشه اسناد اداری مهم شخصی و مالی را که دیگر به آنها نیاز ندارید به روشی که دیگر قابل استفاده نباشد از بین ببرید . اگراین کار را نکنید جنایتکاران به اسم، آدرس و دیگر اطلاعات شما از طریق رسید ها، قبض ها و مدارک مهمی که دور می ریزید، دسترسی پیدا می کنند و از آنها سوء استفاده می کنند.

اسناد اداری که باید از بین بروند شامل موارد زیر می شوند:

- صورت حساب های قدیمی بانکی، مالی و کارت های بانکی قدیمی.
- رسید های قدیمی.
- هر پرسشنامه ای که به طورکامل پر نشده و شامل اطلاعات شخصی شماست.
- هر مرسوله پستی که حاوی اسم و آدرس شما می باشد.

● اطلاعات بانک را به روز کنید

بانک ممکن است نیازداشته باشد در زمان انجام تراکنش هایی که در مقایسه با تراکنش های معمول شما غیر عادی به نظر می رسند، با شما تماس گرفته و برای اطمینان از صحت آن ها برخی ازاطلاعات شخصی شما را جویا شود. این امر می تواند موجب کاهش جرایم مالی شود. بسیار ضروری است که در صورت تغییر اسم، آدرس یا شماره تماس های خود، آن را سریعا به اطلاع بانک برسانید.

●صورت حساب های خود را چک کنید

بسیاری از جرایم مالی تا مدت ها کشف نمی شوند فقط به این دلیل که قربانی از وقوع آنها بی اطلاع است. بنابراین کنترل صورت حساب های بانکی یا هر صورت حساب دیگر پس از دریافت، بسیار ضروری می باشد .باید مطمئن شوید که هرچیزی که ثبت شده است صحت دارد. اگر تراکنشی وجود دارد که از آن بی اطلاع هستید آن را سریعا به اطلاع نزدیک ترین شعبه بانک برسانید.

بسیاری از جرایم مالی تا مدت ها کشف نمی شوند فقط به این دلیل که قربانی از وقوع آنها بی اطلاع است. بنابراین کنترل صورت حساب های بانکی یا هر صورت حساب دیگر پس از دریافت، بسیار ضروری می باشد .باید مطمئن شوید که هرچیزی که ثبت شده است صحت دارد. اگر تراکنشی وجود دارد که از آن بی اطلاع هستید آن را سریعا به اطلاع نزدیک ترین شعبه بانک برسانید.

شما می توانید به روش های مختلف از طریق خود پردازها، سیستم تلفن بانک، سیستم اینترنت بانک و یا مراجعه به شعب از آخرین تراکنش های انجام شده بر روی حساب های شخصی خود آگاه شوید.

●فریب ایمیل ها یا پیامک های دروغین را نخورید

هیچ گاه به ایمیل ها و پیامک های مشکوک یا ناخواسته پاسخ ندهید و هیچگاه برروی لینک ها یا فایل های ضمیمه موجود در این ایمیل های مشکوک کلیک نکنید.

●از کامپیوتر خود محافظت کنید

اگر کامپیوتر شما ایمن نباشد امکان افشا شدن اطلاعات شما وجود دارد. باید بدانید که چگونه از کامپیوتر خود در مقابل تهدیدات محافظت کنید.

قبل از اینکه میز خود را ترک کنید، سیستم خود را قفل نمایید.

با استفاده از یکی از سه روش زیر می توانید سیستم خود را قفل نمایید:

۱ .فشار دادن دکمه هایCtrl+Alt+Delete

۲ .فشار دادن دکمه هایWindows+L

۳ .روی صفحه نمایش سیستم خود راست کلیک نمایید .سپس گزینه New Shortcut را انتخاب و در پنجره ای که ظاهر می شود، متنrundll32.exe user32.dll LockWorkStation را تایپ نمایید. یک Shortcut روی صفحه نمایش شما ظاهر خواهد شد. هر بار که روی این Shortcut دو بار کلیک نمایید، سیستم شما قفل خواهد شد.

●Firewall

نرم افزاری است که کامپیوتر شما را در مقابل حملات اینترنتی محافظت می کند. باید بر روی هر کامپیوتری که برای اتصال به اینترنت از آن استفاده می کنید firewall نصب شده باشد. به شما پیشنهاد می کنیم که firewall خود را طوری تنظیم کنید که تبادل اطلاعات از طریق کامپیوتر شما را کنترل کند.

●AntiVirus

حتما از یک آنتی ویروس بر روی سیستم خود استفاده نمایید و آن را به طور مرتب به روز رسانی کنید. توجه داشته باشید که آنتی ویروس های به روز رسانی نشده ویروس های جدید را شناسایی نخواهند کرد.

●به روز رسانی سیستم عامل

گاهی وجود حفره امنیتی در سیستم عامل ها باعث ورود انواع ویروس ها به سیستم شما خواهد شد. به تدریج این حفره های امنیتی شناسایی می شوند و شرکت های سازنده برای رفع آن ها Patch هایی تهیه و در اختیار مشتریان قرار می دهند. حتماً جدیدترین Patch ها را روی سیستم خود نصب نمایید تا از حملات ویروس ها یا بدافزارهای جدید در امان بمانید.

●شناسه کاربری

هرگز از اطلاعات شخصی خود مانند شماره تلفن همراه، نام و نام خانوادگی در شناسه کاربری خود استفاده نکنید. با این کار شما یکی از عوامل احراز هویت را به راحتی در دسترس نفوذگران قرار خواهید داد و کار را برای فعالیت های مخرب آن ها راحت خواهید کرد. فقط کافی ا ست نفوذگران رمز عبور شما را حدس بزنند تا بتوانند به حساب شما دسترسی داشته باشند.

●رمز عبور

رمزهای عبور بخش مهمی از سرویس های بانکی الکترونیکی می باشند و در حقیقت در خط مقدم حفاظت از حساب های کاربری در سرویس های مذکور قرار می گیرند. یک کلمه عبور نا مناسب ممکن است منجر به کلاهبرداری های مالی بزرگی شود.

بهترین رمز عبور، رمزی است که شما آن را به راحتی به خاطر می سپارید ولی دیگران نمی توانند آن را حدس بزنند. وقتی که رمز عبور خود را انتخاب کردید آن را به طور منظم عوض نمایید. اگر برای یک سال است که از یک رمز عبور استفاده می کنید الان زمانی است که باید آن را تغییر دهید.

هرگز رمز عبور خود را در اختیار دیگران نگذارید و هیچ گاه آن را جایی ننویسید یا در کامپیوتر خود ذخیره نکنید.

در انتخاب رمز عبور مناسب به موارد زیر دقت کنید:

- هیچ گاه برای رمز عبور خود از اطلاعات شخصی مانند اسم، تاریخ تولد، شماره موبایل و ... استفاده نکنید.
- رمزهای عبور پیش فرض را پس از اولین ورود به سیستم تغییر دهید.

- بهتر است رمزهای عبور در سیستم های مختلف با یکدیگر متفاوت باشند.
- هر چقدر رمز عبور طولانی تر باشد امنیت آن بیشتر است (حداقل ۸ کاراکتر.)
- از رمز های عبور ترکیبی استفاده کنید که شامل حروف کوچک، حروف بزرگ، ارقام و نشانه ها شود. مانند: A۱ ¤ Gw۴ ۵S۱
- سعی کنید در رمز عبور حداقل یک بار از Space استفاده نمایید.
- حداقل هر ۳ ماه یک بار بنا به دفعات استفاده، رمز عبور خود را تعویض کنید که البته تغییر یک ماهه توصیه می شود.
- کلمات عبور خود را با هیچ کس درمیان نگذارید. با تمام رمزهای عبور خود به عنوان اطلاعات حساس محرمانه برخورد کنید.

●استفاده از اینترنت در مکان های عمومی

امنیت شبکه های بیسیم یا کامپیوترهایی که در مکان های عمومی مانند هتل ها، کتابخانه ها یا کافی نت ها قرار دارند تضمین شده نیست. به شما پیشنهاد می کنیم که در چنین شرایطی از حساب های بانکی خود استفاده نکنید. ترجیحاً تا جایی که می توانید ازسایت های کمتری بازدید کنید و زمان کمتری در این موقعیت ها قرار گیرید.

همیشه نکات زیر را به خاطر بسپارید:

- تا آنجا که ممکن است هنگامی که از شبکه های بیسیم یا کامپیوترهای عمومی استفاده می کنید اطلاعات امنیتی خود مانند رمز عبور را وارد نکرده و تغییر ندهید.
- هیچ گاه هنگامی که در چنین شرایطی قرار دارید، اطلاعات حساب ها یا کارت های بانکی خود را در یک سایت فروش اینترنتی وارد نکنید.
- همیشه مراقب کسانی که در اطراف شما هستند باشید.

●امنیت شخصی

- باید مراقب افراد اطراف خود در زمانی که از دستگاه های خود پرداز استفاده می کنید، باشید.
- هنگام استفاده از دستگاه خود پرداز نزدیک به آن بایستید و روی صفحه کلید را بپوشانید به طوری که کسی رمز عبور شما را در هنگام وارد کردن نبیند.

- کمک افراد غریبه را نپذیرید و اجازه ندهید کسی شما را گیج کند.
- اگر هنگامی که از دستگاه های خود پرداز استفاده می کنید شخصی مشکوک به نظر رسید یا به شما نزدیک شد عملیات خود را لغو کنید و از آن مکان دور شوید.
- پس از تکمیل عملیات، قبل از اینکه دستگاه خود پرداز را ترک کنید، سریعا پول و کارت خود را بردارید.
- در پایانه های فروشگاه ها زمانی که رمز عبور خود را وارد می نمایید مراقب باشید که کسی از پشت سر شما رمز عبور را نبیند.
- کمک افراد غریبه را نپذیرید و اجازه ندهید کسی شما را گیج کند.
- اگر هنگامی که از دستگاه های خود پرداز استفاده می کنید شخصی مشکوک به نظر رسید یا به شما نزدیک شد عملیات خود را لغو کنید و از آن مکان دور شوید.
- پس از تکمیل عملیات، قبل از اینکه دستگاه خود پرداز را ترک کنید، سریعا پول و کارت خود را بردارید.
- در پایانه های فروشگاه ها زمانی که رمز عبور خود را وارد می نمایید مراقب باشید که کسی از پشت سر شما رمز عبور را نبیند.
- اطراف دستگاه خود پرداز به خصوص قسمت های کارت خوان و صفحه کلید را کنترل کنید چرا که ممکن است افراد سودجو برای دزدیدن اطلاعات شما به نصب دوربین، صفحه کلید جعلی یا کارت خوان جعلی اقدام نموده باشند.
- ازلپ تاپ، تلفن همراه و دیگر وسایل الکترونیکی خود محافظت کنید.
- به یاد داشته باشید که همواره مراقب لپ تاپ و تلفن همراه خود باشید. آنها را همیشه در دسترس خود نگه دارید به خصوص زمانی که درمسافرت هستید.
- هیچ گاه لپ تاپ خود را روشن و قفل نشده درمکان های عمومی رها نکنید.
- هیچ گاه درمورد مسائل محرمانه درمکان های عمومی صحبت نکنید.
- تلفن همراه و لپ تاپ خود را هنگامی که از آنها استفاده نمی کنید قفل کنید.

بسیاری از مشتریان، اینترنت را فضای مناسبی برای تعاملات تجاری نمی دانند و حتی هویت یک کسب و کار در فضای اینترنت [۵۲] را به رسمیت نمی شناسند. در چنین شرایطی ایجاد اطمینان در مشتریان بالقوه و جلب اعتماد آنان برای عرضه کنندگان کالا یا خدمات در بازار اینترنت دشوار است.

[۵۲] Web Site

مخفی کردن هویت در اینترنت

Hide IP NG نرم افزاری است که امنیت اینترنتی شما را تامین می کند و در هنگام گشت و گذار در اینترنت IP[۵۳] شما را مخفی می نماید. توسط این نرم افزار هیچ نگرانی نخواهید داشت و این نرم افزار تمام کارهای لازم برای مخفی ماندن شما را انجام می دهد. همچنین این نرم افزار ID شما را در اینترنت مخفی نگاه می دارد و اطلاعات خصوصی شما را غیر قابل دسترس می نماید و از دریافت Spam و ایمیل های ناخواسته تبلیغاتی که از طرف سایت ها و یا کمپانی هایی که ایمیل شما را در اختیار دارند جلوگیری می نماید . این نرم افزار با مخفی نمودن IP ,کامپیوتر شما را از حملات هکرها در امان نگاه می دارد. بسیاری از وب سایت ها امکان استفاده ی بیش از یک IP را از اطلاعات درونشان نمی دهند، توسط این نرم افزار و با توانایی تعویض لحظه ای IP دیگر این مشکل را نخواهید داشت.

[۵۳] نشانی پروتکل اینترنت (Intenten Protocol Address) یا به اختصار IP شماره ای است که به هر کامپیوتر متصل به ابنترنت اختصاص داده می شود تا بتوان به کمک آن شماره به کامپیوتر مربوطه دسترسی داشته و تبادل اطلاعات نمود .

نتیجه گیری

با توجه به امکانات تهیه شده از سوی بانک ملت جهت کاهش اشتباهات پیش آمده از سوی همکاران لازم است که کلیه همکاران از این امکانات استفاده کرده تا زمینه های مساعد جهت سوء استفاده افراد سودجو به صفر برسد همچنین استفاده بانک از روشهای ترکیبی و مضاعف می تواند به این امر کمک کند .

منابع

مبانی امنیت شبکه ،گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف

Fundamentals of Network Security by Eric Maiwald

Weis, Stephen A. (2007), *RFID (Radio Frequency Identification): Principles and Applications*

Daniel M. Dobkin, *The RF in RFID: Passive UHF RFID In Practice*, Newnes 2008

Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". *Communications of the ACM*

Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publications.

بانکداری عملیاتی ؛اداره کل آموزش بانک ملت،تدوین : پیمان طوبایی

TCP/IP ترجمه :مهندس کیادی مقدم

بانکداری الکترونیکی ؛ حسین عباسی نژاد

مدیریت بانکداری الکترونیکی ؛ مهندس فرنود حسنی , سهیلا سلطانی و فرشته ضرابیه

پول شوئی الکترونیکی ؛ امیر حسین جلالی فراهانی

دانش مدیریت بانکی ؛مرکز تحقیقات و مدیریت بانک ملت

قانون مدنی جلد اول ، دوم وسوم

قانون تجارت الکترونیکی

حقوق بانکی پیشرفته ؛ اداره کل حقوقی بانک ملت

راهنمای سامانه متمرکز بانک ملت Core Banking

راهنمای سامانه فرانام

مجلات پرتو بانک ملت

سایت بانک ملت http://bankmellat.ir

سایت بانکداری الکترونیکی بانک ملت https://ebanking.bankmellat.ir

سایت اینترانتی بخشنامه های بانک ملت http://bakhshnameh.bm

سایت اینترانتی فن آوری بانک ملت http://it.bm