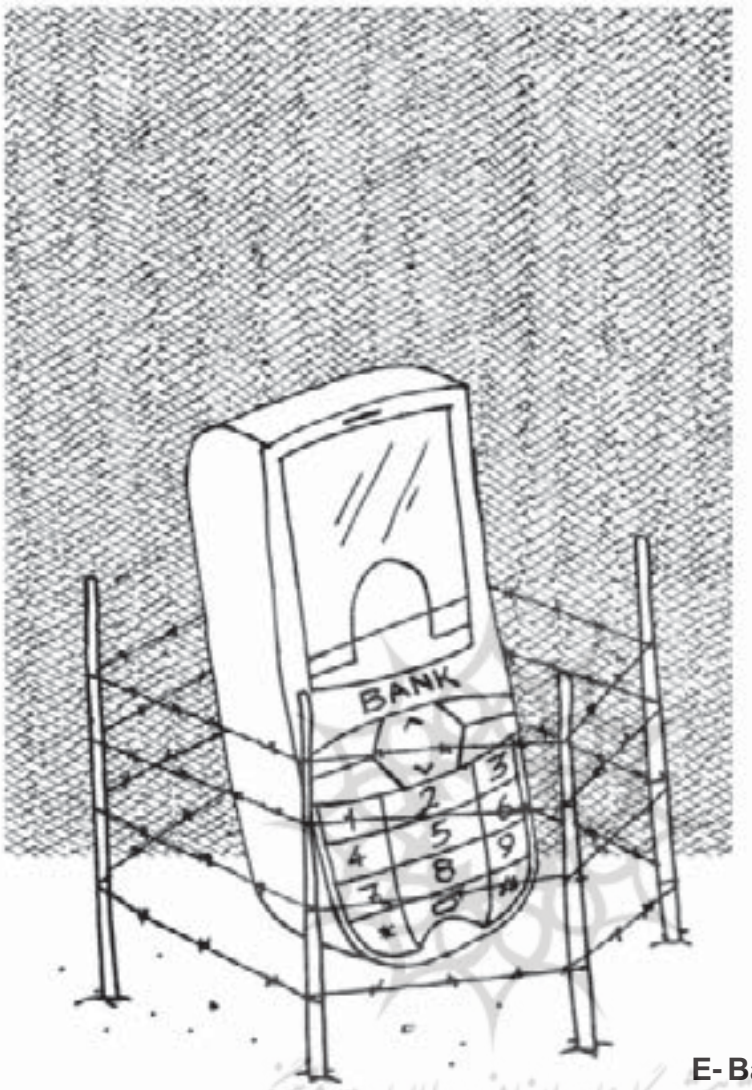

بانکداری الکترونیک در انتظار رفع ابهامات و مخاطرات

منبع: مجله اینترنتی E- Banking
مترجم: سید حسین علوی لنگرودی

بانکداری موبایل

بانکداری موبایل یا همان ارائه خدمات بانکی از طریق شبکه تلفن همراه، برآیند و محصول طبیعی پیشرفت‌های تکنولوژیکی در عرصه ارتباطات و اطلاعات تلقی می‌شود و یکی از حوزه‌هایی است که دو قلمرو بانکداری و وسایل ارتباطی را به هم پیوند می‌زند. تلفن‌های همراه، با رشد و پیشرفت خیره کننده‌ای که طی چند سال اخیر داشته‌اند، توانسته‌اند مسیر جدیدی را برای ارائه خدمات مالی و بانکی از سوی بانک‌ها و مؤسسات مالی به مشتریانشان در اقصی نقاط جهان، به وجود آورند.

بانکداری موبایل، جدیدترین موج از امواج انقلابی و سهمگینی است که صنعت بانکداری را در دهه‌های اخیر، دگرگون کرده است. این جریان با اختراع و گسترش دستگاه‌های خود پرداز (ATM) در دهه ۱۹۸۰، آغاز و با توسعه خدماتی چون بانکداری تلفنی و بانکداری آن لاین و اینترنتی ادامه یافت و هم اکنون به صورت بانکداری همراه، نمود و ظهور یافته است. برخی از کارشناسان بر این اعتقادند که با منتقل کردن کارایی‌های گسترده شبکه اینترنت به شبکه‌های موبایل و تجهیز گوشی‌های جدید با امکانات اتصال نامحدود و سریع و کم هزینه به اینترنت، می‌توان امیدوار بود که بانکداری همراه به ترکیبی کامل و بی نظیر از مزایا و امکانات بانکداری اینترنتی و تلفن همراه، به صورت توأمان، تبدیل شود.

تقاضا برای برخورداری از خدمات مالی و بانکی تلفن همراه در سال‌های نخستین قرن۲۱، به شدت افزایش یافت که این امر، معلول عوامل متعددی بود که برخی از آنها عبارتند از: سهولت و سادگی استفاده از تلفن‌های همراه برای انجام دادن کارهای بانکی، در دسترس بودن و همگانی بودن تلفن‌های همراه، ظهور پدیده خارق العاده‌ای به نام «سرویس پیام کوتاه» یا SMS و پیشرفت‌های سریع و شگفت انگیز در بخش طراحی وساخت گوشی‌های تلفن همراه.

نیمه تاریک بانکداری موبایل

با این همه عرصه بانکداری همراه و خدمات رسانی بانکی از طریق تلفن‌های همراه، عاری از ابهامات و مخاطرات خطرناک و بازدارنده نبوده و نیست و موارد متعددی از ناکامی و عدم موفقیت بانک‌ها در خدمات‌رسانی مالی تلفن همراه در سرتاسر جهان به چشم می‌خورد که نتیجه تأثیر گذاری منفی و نامطلوب عوامل بازدارنده و مخربی هستند که در ادامه به آنها اشاره خواهیم کرد.

یکی از دلایل اصلی ناکارآمدی خدمات بانکی همراه، برخورد احساسی و آرمان گرایانه مشتریان بانک‌ها و حتی مدیران و کارمندان بانک‌ها با این حوزه جدید از خدمات رسانی مالی و بانکی نوین است. اغلب کارکردهای بانکداری همراه، آنچنان که بسیاری از مشتریان بانک‌ها فکر می‌کنند، مورد استفاده عموم مشتریان نبوده و کاربران و متقاضیان خاصی را می‌طلبد. برخی از این نوع خدمات نیز فقط به درد آن دسته از مشتریان بانک‌ها می‌خورد که دارای تحصیلات عالی و حرفه‌ای در حوزه‌های مالی و بانکی هستند. پایین بودن درآمد حاصل از ارائه این نوع خدمات نوین برای بانک‌ها و مؤسسات مالی و استقبال نکردن مطلوب و کافی مشتریان از این خدمات (در برخی موارد)، یکی از عوامل بازدارنده و منفی محسوب می‌شود.

برخی از کارشناسان بر این اعتقادند که با منتقل کردن کارایی‌های گسترده شبکه اینترنت به شبکه‌های موبایل و تجهیز گوشی‌های جدید با امکانات اتصال نامحدود و سریع و کم هزینه به اینترنت، می‌توان امیدوار بود که بانکداری همراه به ترکیبی کامل و بی‌نظیر از مزایا و امکانات بانکداری اینترنتی و تلفن همراه، به صورت توأمان، تبدیل شود

به طور کلی، اگر مزایای خاص و جالبی چون پرداخت‌ها از طریق تلفن همراه را از قلمرو بانکداری همراه، حذف کنیم، این قلمرو نوظهور و پرتکاپو، از رونق خواهد افتاد و به قهقرا کشیده خواهد شد. وجود رقیب قدرتمند و پر طرفداری به نام «بانکداری اینترنتی» موجب شده تا اکثر طرفداران استفاده از ابزارهای نوین خدمات مالی و بانکی، به سمت اینترنت و بانک‌های اینترنتی گرایش یابند و این یعنی کم شدن گرایش به سمت بانکداری همراه.

علت چیست؟

مهم‌ترین علت ناکامی بانکداری موبایل در برخی موارد، به مسائل امنیتی و کنترلی مربوط می‌شود. در سال‌های اخیر، موارد متعددی از به سرقت رفتن اطلاعات محرمانه کاربران خدمات بانکداری همراه و اختلاس از طریق همراه، گزارش شده است که به علت رشد فزاینده این موارد، اعتماد عمومی به خدمات بانکداری همراه در برخی کشورها، به شدت کاهش یافته است. لو رفتن شماره‌های شناسایی و پین کدها، موجب افشا شدن اطلاعات مالی افراد و افزایش احتمال برداشت‌های غیر قانونی از حساب آنها می‌شود و ضرر و زیان هنگفتی را برای مشتریان و بانک‌ها، به دنبال دارد. در سال ۲۰۰۶، بیش از ۱۰ میلیون آمریکایی، قربانی افشای ناخواسته اطلاعات مالی خود از طریق تلفن‌های همراه خود شدند که بخش عمده موارد لو رفتن اطلاعات مالی، به واسطه کپی برداری غیر قانونی از سیم کارت‌های مشتریان و سوء استفاده از حساب‌های بانکی همراه افراد به وجود آمده است. بنا به نتایج پژوهشی که اخیراً توسط کمیسیون تجارت فدرال آمریکا (FTC) به عمل آمده است، بیش از ۱۳ درصد قربانیان افشای غیرقانونی اطلاعات مالی، مدعی هستند که اطلاعات شخصی و محرمانه آنها، به ویژه، شماره‌های شناسایی و رمز عبور تلفن همراه آنها، در زمان استفاده از خدمات بانکی همراه، به ویژه، خرید از طریق کارت‌های اعتباری یا پرداخت‌های همراه، لو رفته و خسارات فراوانی را به آنها و بانک‌هایی که حساب‌های همراه را در اختیارشان قرار داده‌اند، وارد آورده است. بیش از ۵۰ درصد این قربانیان نیز نسبت به علت لو رفتن اطلاعات شخصی و رمز عبور همراه خود، اظهار بی اطلاعی کرده و مدعی‌اند که بانک‌ها مسئول افشای

اطلاعات محرمانه آنها بوده‌اند.

براساس پژوهش FTC ، بیش از ۹۵ درصد موارد به سرقت

یک سری رمزهای عبور و کدهای دیجیتال، در زمان افتتاح حساب آن لاین یا تلفن همراه، در اختیار مشتریان متقاضی برخورداری از خدمات بانکداری الکترونیک قرار می‌گیرد که آنها را قادر می‌سازد تا هر زمان که می‌خواهند و فقط با وارد کردن این اطلاعات خاص، وارد سیستم شده و از خدمات موجود استفاده کنند

رفتن شماره‌های شناسایی و رمز عبور، ناشی از بی‌دقتی کاربران تلفن‌های همراه در استفاده از خدمات بانکداری همراه، به ویژه در زمان انجام دادن پرداخت‌های همراه، بوده است. امروزه، اغلب کاربران تلفن‌های همراه و اینترنت، از افشای اطلاعات محرمانه و شخصی خود در هنگام کار با تلفن همراه یا اینترنت، اِبایی ندارند و به آسانی رمز عبور و کدهای شناسایی تلفن همراه یا رایانه شخصی خود را افشا می‌کنند که این امر، دست سارقان آنلاین برای سوء استفاده از حساب‌های ویژه بانکداری همراه یا بانکداری اینترنتی را باز می‌گذارد. متأسفانه،سارقان اینترنتی و تلفن همراه، از سادگی و ناآگاهی کاربران اینترنت و تلفن همراه، نهایت سوء استفاده را می‌کنند و با طراحی وب سایت‌ها و شبکه‌های داخلی تلفن همراه، کاربران را به سمت افشای اطلاعات محرمانه و شخصی خود، از جمله رمز عبور و شماره‌های شناسایی، سوق می‌دهند و سپس با ایجاد یک بانک اطلاعاتی غیر قانونی، نسبت به برداشت‌های غیر قانونی از حساب‌های اینترنتی و همراه افراد اقدام کرده و میلیون‌ها دلار پول را به صورت غیرقانونی از حساب افراد برداشت وبه حساب‌های شخصی خود منتقل می‌کنند. بر اساس نتایج به دست آمده از پژوهش FTC، از هر ۷۰۰ عملیات بانکی تلفن همراه در آمریکا، یک عملیات به صورت غیر قانونی و بدون آگاهی صاحب حساب بانکی تلفن همراه، انجام می‌گیرد.

سرقت الکترونیکی چیست؟

سرقت الکترونیکی از تلفن‌های همراه و سوء استفاده از شماره‌های شناسایی و رمز ورود به سیستم، یک جرم مالی جدید محسوب می‌شود که در آن، سارقان خود را به جای صاحب تلفن همراه و حساب تلفن همراه، جا زده و از این طریق، اطلاعات کلیدی و محرمانه داخل گوشی از جمله پین کدها، شماره حساب‌های بانکی، رمز عبور کارت‌های اعتباری و شماره گواهینامه رانندگی صاحب آن را برداشت می‌کنند. نوع دیگری از سرقت‌های الکترونیک نیز وجود دارد که در آن، سارق با نفوذ به سیستم کارت‌های اعتباری آن بانک راه یافته و از حساب آنها، به طور غیر قانونی، پول برداشت می‌کند و از این طریق، میلیون‌ها و یا شاید، میلیاردها دلار به مشتریان بانک و خود بانک، زیان وارد می‌کند.

متأسفانه، در بسیاری از کشورهای جهان، حتی در کشورهای صنعتی، قوانین و مقررات جامع و قاطعی برای برخورد با سارقان الکترونیک از بانک‌ها و حساب‌های بانکی، وجود ندارد و اگر هم وجود داشته باشد، به درستی، به مرحله اجرا در نمی‌آید. به عنوان مثال، اگر از حساب الکترونیکی یک شخص، مبلغی بیش از حد مجاز برداشت شود (ولو این عمل به صورت مخفیانه و بدون آگاهی صاحب حساب باشد)، مقامات قضایی، تا زمان پیدا نشدن عامل اصلی این اقدام، یعنی همان سارق الکترونیک، فرد یا افراد صاحب الکترونیک را مسئول و متهم می‌شناسد، مگر اینکه بی‌گناهی او برای دادگاه محرز شود.

خود بانک‌ها، مؤسسات مالی و شرکت‌های ارائه دهنده کارت های اعتباری و حساب‌های بانکی همراه نیز فاقد یک راهبرد مدون و کامل برای مقابله با این مشکل هستند و از نظر اغلب آنها، سرقت‌های الکترونیکی از حساب‌های الکترونیکی (اینترنتی و تلفن همراه) امری مرتبط با مشتریان آنهاست و به آنها ربطی ندارد و لذا، بانک نباید در قبال وقوع سرقت‌های الکترونیکی، پاسخگو باشد. به عقیده بانکداران، سرقت شماره‌های شناسایی و رمزهای عبور، به واسطه تساهل و سستی خود کاربران حساب‌های الکترونیکی به وقوع می‌پیوندد و مسئولیتی از این بابت، متوجه بانک‌ها نیست. در چنین وضعیتی تنها سر مشتریان بی‌گناه و بی‌خبر از همه جا، بی کلاه می‌ماند و کسی پاسخگوی شکایات آنها نیست.

قانونگذاران باید وارد کارزار شوند

برای جلوگیری از گسترش سرقت اطلاعات مالی افراد از طریق

نفوذ به تلفن همراه یا حساب های اینترنتی، قانونگذاران و سیاستگذاران عرصه‌های پولی و بانکی باید یک سری الزامات قانونی را با هدف پیشبرد فرایندهای ضد اختلاس و کلاهبرداری الکترونیک به مرحله اجرا در آورند. آنها باید بانک‌ها را موظف کنند تا در زمان افتتاح حساب‌های الکترونیکی، اعم از اینترنتی و تلفن همراه، یک شماره شناسایی اضطراری به مشتری اختصاص دهند که با استفاده از آن، ضریب امنیتی حساب‌های الکترونیکی به نحو چشمگیری افزایش یابد و از وارد آمدن ضرر و زیان‌های گسترده بر مشتریان و کاربرانی که مورد دستبرد الکترونیکی قرار گرفته‌اند، جلوگیری کنند. با افزایش ضریب امنیتی حساب‌های بانکی همراه، هکرها، کارمندان متخلف بانک‌ها و سایر اشخاصی که قصد دارند با نفوذ به حساب‌های الکترونیکی افراد، از حساب بانکی آنها سوء استفاده کنند و پول برداشت نمایند، در رسیدن به اهداف پلید خود، ناکام خواهند ماند.

در سال‌های اخیر، موارد متعددی از به سرقت رفتن اطلاعات محرمانه کاربران خدمات بانکداری همراه و اختلاس از طریق همراه، گزارش شده است که به علت رشد فزاینده این موارد، اعتماد عمومی به خدمات بانکداری همراه در برخی کشورها، به شدت کاهش یافته است

علاوه بر این، باید یک سری آموزش‌های کلی و ابتدایی را در مورد نحوه مراقبت اطلاعات محرمانه موجود در حساب‌های بانکی الکترونیک و راه‌های جلوگیری از به سرقت رفتن یا لو رفتن شماره‌های شناسایی و رمزهای عبور مربوط به حساب‌های همراه و اینترنتی، به مشتریانی که متقاضی افتتاح حساب‌های الکترونیکی هستند، ارائه کرد. البته چنین فرایندهایی از ابعاد مختلف، برای بانک‌ها، مؤسسات مالی و شرکت‌های ارائه دهنده خدمات کارت های اعتباری، مسئولیت آور و پر درد سر خواهد بود و هزینه‌های سنگینی را برای آنها به بار خواهد آورد. از سویی دیگر، هر گونه نفوذ احتمالی به سیستم‌های الکترونیکی بانک و به سرقت رفتن اطلاعات ذخیره شده در بانک اطلاعاتی آن، به معنای وارد آمدن زیان‌های فوق العاده سنگینی به بانک خواهد بود و حیثیت بانک‌ها را در اجتماع تخریب خواهد کرد.

هم اکنون، بسیاری از شرکت‌های بزرگ آمریکایی، از جمله مایکروسافت، آمازون و ebay دست به دست هم داده‌اند و ائتلافی را بر ضد سرقت‌های الکترونیکی به وجود آورده‌اند. این ائتلاف با هدف تشدید مبارزه عمومی با سرقت‌های الکترونیکی از طریق دادن آموزش‌های جامع به کاربران حساب‌های اینترنتی و تلفن همراه و مستحکم کردن سیستم‌های خدمات‌رسانی مالی وبانکی همراه و اینترنتی شکل گرفته است و امید می‌رود تا با افزایش ارتباطات میان بانکداران، متخصصان الکترونیک و امنیت سیستم‌ها و البته، قانونگذاران و سیاستگذاران عرصه‌های بانکی و اقتصادی، تا حد زیادی از موارد اختلاس و سوء استفاده از حساب‌های الکترونیک افراد، کاسته شود. تحقق چنین اهدافی هم به سود مشتریان بانک‌ها - که از حساب‌های الکترونیکی برای انجام دادن مبادلات مالی و عملیات بانکی خود بهره می‌برند - خواهد بود و هم از بانک‌ها در برابر نفوذ سارقان الکترونیکی و هکرها محافظت به عمل می‌آورد.

ریسک‌های بانکداری الکترونیک

در این بخش، به برخی از مخاطرات و نقاط ضعف الگوهای بانکداری الکترونیک به طور عام، و بانکداری همراه، به طور خاص خواهیم پرداخت و روش‌های نفوذ مهاجمان به شبکه‌های مالی تلفن همراه را به اختصار شرح خواهیم داد.

یکی از مهم‌ترین و در عین حال خطرناک‌ترین نقطه ضعف بانکداری الکترونیک، ناتوانی سیستم‌های بانکی در شناسایی کامل و دقیق مشتریان صاحب حساب الکترونیک است. سیستم‌های بانکداری همراه به گونه‌ای طراحی شده‌اند که با وارد شدن یک یا چند کاراکتر (از قبیل شماره تلفن همراه، شماره شناسنامه یا گواهینامه فرد صاحب حساب) به طور اتوماتیک، فرد وارد کننده این اطلاعات را به عنوان صاحب حساب شناسایی کرده و هر گونه خدماتی را که مورد تقاضای او باشد، در اختیار او قرارمی‌دهد. به عنوان مثال، در یکی از بزرگ‌ترین کلاهبرداری‌های الکترونیکی در آمریکا، یک سارق الکترونیکی با وارد کردن شماره تلفن همراه و پین کد یک میلیونر آمریکایی، چندین میلیون دلار از حساب همراه او برداشت کرد. او پس از دستگیری

توسط پلیس، اعترافاتی کرد که دست اندرکاران سیستم‌های امنیتی تلفن همراه را به حیرت انداخت. او به پلیس گفت که پس از به دست آوردن اطلاعاتی مختصر در مورد قربانی‌اش، به سیستم بانکداری همراه بانکی که آن فرد در آنجا حساب داشت، وارد شده و تقاضای اطلاع یافتن از موجودی حساب کرد که فرمانی است کاملا عادی ورایج. سیستم بانک نیز که او را به عنوان فرد صاحب حساب شناسایی کرده بود، لیستی از خدمات و عملیات پیشنهادی را برای استفاده آن کاربر ارائه کرد که همین مسأله، امکان دسترسی مستقیم و نامحدود فرد سارق به حساب همراه مورد نظر را فراهم کرد.

یکی دیگر از ریسک‌های موجود در بانکداری همراه، فرستاده شدن پیام‌های کوتاه (SMS) ساختگی و جعلی برای فرد صاحب حساب همراه با هدف کسب اطلاعات شخصی و شماره‌های شناسایی اوست. این پیام‌ها، به ظاهر از سوی بانک یا مؤسسه مالی که فرد در آن حساب همراه افتتاح کرده است، ارسال می‌شوند و حاوی پرسش‌هایی مربوط به اطلاعات شخصی برای تکمیل پرونده بانکی او می‌شود، حال آنکه واقعیت امر، چیز دیگری است و هدف کسب اطلاعات برای سوء استفاده از حساب تلفن همراه است. صاحبان حساب‌های تلفن همراه باید بدانند که این ریسک هنگامی ابعاد جدی‌تر و خطرناک‌تری به خود می‌گیرد که نفوذ اولیه مهاجم یا مهاجمان باعث لو رفتن اطلاعات کلیدی از جمله صورت موجودی و کدهای امنیتی حساب همراه می‌شود که همین امر، راه را برای حملات و سرقت‌های بعدی از حساب مورد نظر، هموار می‌سازد.

برای جلوگیری از وقوع چنین سوء استفاده‌هایی، طراحان بانکداری تلفن همراه باید سیستمی را ایجاد کنند که هر گونه ارائه خدمات بانکی تلفن همراه را موکول و منوط به دریافت یک سری اطلاعات خاص و سرّی کنند که در زمان افتتاح حساب همراه توسط فرد متقاضی، از او جمع آوری می‌شود (شبیه همان فرایندی که در زمان ایجاد پست الکترونیکی (e-mail) روی می‌دهد و سؤالاتی از قبیل «نام حیوان خانگی شما چیست؟» از کاربر پرسیده می‌شود. چنین تمهیداتی می‌تواند تا حد زیادی از سوءاستفاده‌های احتمالی از حساب‌های بانکی تلفن همراه از طریق ارسال پیام‌های جعلی به نیابت از بانک جلوگیری کند.

برای کسب اطلاعات بیشتر در این مورد به سایت اینترنتی زیر رجوع کنید: http://www.bulkservice.com

مدیریت ریسک‌های بانکداری الکترونیک

با اجرایی شدن رسمی و فراگیر مفاد عهدنامه باسل ۲ از اول ژانویه سال ۲۰۰۷، بانک‌ها و مؤسسات مالی جهان، موظف به رعایت اصول و مقررات پیشنهادی در این عهد نامه شده‌اند. باسل ۲ با هدف هماهنگ سازی و بهسازی رویکردها و فرایندهای مرتبط با مدیریت ریسک در ابعاد و جنبه‌های مختلف آن، تنظیم شده که بخشی از آن به نحوه مقابله با ریسک‌های بانکداری الکترونیک اختصاص یافته است.

در یکی از بندهای عهدنامه باسل ۲ تحت عنوان «اصول مدیریت ریسک برای بانکداری الکترونیک» به چهارده ریسک اصلی و رایج در حوزه بانکداری الکترونیک اشاره و رهنمودهایی برای غلبه بر این ریسک‌ها ارائه شده است. این رهنمودها، بسیار جامع و کاربردی

است و برای تمام بانک‌هایی که خدمات بانکداری الکترونیک را به مشتریان خود عرضه می‌دارند، مفید خواهد بود. در عهدنامه باسل ۲ به دفعات به مبحث بانکداری الکترونیک و مخاطرات آن اشاره شده است. کمیته ناظر بر تصویب عهدنامه باسل ۲ بر این مسأله تأکید دارد که همه بانک‌ها و مؤسسات مالی فعال در حوزه بانکداری الکترونیک باید هوشیار باشند که ریسک‌های مالی و حقوقی متعددی به همراه پیشرفت‌های تکنولوژیکی ناشی از انقلاب اطلاعات در قالب اینترنت و همراه، ظهور کرده‌اند که بی‌توجهی به آنها می‌تواند پیامدهای وخیمی را برای بانک‌ها و مؤسسات مالی به همراه داشته باشد. با توجه به رشد چشمگیر و روزافزون وسایل ارتباطی و تحولات بی‌سابقه و سریع در دستگاه‌های ارتباطی مانند تلفن همراه و کامپیوترهای جیبی، مدیران و سیاستگذاران بانک‌ها باید در فواصل کوتاه به بازسازی و نوسازی راهبردهای مدیریت ریسک خود اقدام کنند تا از تبعات منفی تأثیر گذاری ریسک‌های جدی بانکداری الکترونیک برای خود و مشتریان خود در امان باشند.

اگرچه بسیاری از اصول و رهنمودهای مدیریت ریسک‌های سنتی در مورد بانکداری الکترونیک نیز قابل اجرا و اثر بخش است، اما ماهیت پیچیده و دگرگون ابزارهای نوین خدمات رسانی مالی و بانکی از قبیل اینترنت و تلفن همراه باعث شده است که ریسک‌هایی حول فعالیت‌ها بانکی نوین، پدیدار شوند که تاکنون سابقه نداشته‌اند و مقابله با آنها از طریق پیاده کردن روش‌های سنتی مدیریت ریسک، امکان‌پذیر نیست. همین سرعت بالا و خیره کننده تحولات و پیشرفت‌ها در طراحی و ساخت ابزارهای جدید بانکداری، لزوم تجدید نظر پیاپی و سریع در سیاست‌های مدیریت ریسک بانک‌ها را به بانکداران گوشزد می‌کند. نوآوری‌های سریع و متعدد در حیطه خدمات‌رسانی بهتر، بیشتر و متنوع‌تر به مشتریان و استفاده از ابزارهای جدیدتر برای ارائه خدمات بانکی به مشتریان و بی‌نیاز کردن آنها برای حضور فیزیکی در شعب بانک‌ها، باعث شده است تا نیاز مبرمی به شناسایی و اجرای راهبردهای چند بعدی و پیچیده‌ای برای کنترل و مدیریت ریسک‌های بانکی، احساس شود و این به معنای لزوم تنظیم و پیاده کردن عهدنامه‌های باسل متعدد و متغیر در طول زمان است.

کمیته تصویب کننده عهدنامه باسل از کلیه بانکداران و نهادهای ناظر بر فعالیت بانک‌ها در سطوح ملی و بین المللی می‌خواهد تا در مواردی که تغییرات خاصی در ماهیت ریسک‌های بانکداری الکترونیک به وجود می‌آید، دست به عمل بزنند و راهبردها و اصول مدیریت ریسک خود را با این تغییرات تطبیق دهند.

به طور کلی، اصول چهارده گانه مدیریت ریسک‌های بانکداری الکترونیک به سه بخش اصلی تقسیم می‌شوند که عبارتند از: ۱) مسئولیت‌های هیأت مدیره و مدیریت، ۲) کنترل‌های امنیتی و ۳) مدیریت ریسک‌های حقوقی و اعتباری که به شرح هر سه بخش می‌پردازیم:

۱) مسئولیت هیأت مدیره:

بر اساس مفاد عهد نامه باسل ۲، اعضای هیأت مدیره و مدیریت ارشد بانک‌ها و مؤسسات مالی ارائه دهنده خدمات بانکداری الکترونیک، موظف‌اند اطمینان حاصل کنند که رویکردها، سیاست‌ها و راهبردهای بانک و مؤسسه مالی تحت مدیریت آنها در بخش مدیریت، اهداف

راهبردی سازمان بوده و از سلامت و استحکام کافی برخوردار باشند. بر این اساس، هیأت مدیره و مدیریت ارشد بانک‌ها، به عنوان مسئول مستقیم و اصلی پیشنهاد و اجرایی کردن این راهبردها و سیاست‌ها، شناخته می‌شوند و موظف‌اند تا زمانی که از مناسب و بی‌خطر بودن یک محصول بانکی نوین اطمینان حاصل نکرده‌اند، از عملیاتی شدن آن جلوگیری کنند، مگر اینکه تمهیدات و پیش بینی‌های مربوط به ریسک‌های احتمالی را از قبل اندیشیده باشند.

کمیته تصویب کننده عهدنامه باسل ۲ به هیأت مدیره و مدیریت ارشد بانک‌ها و مؤسسات مالی مشتاق ارائه خدمات بانکداری الکترونیک هشدار می‌دهد که دچار کوته بینی و دست کم گرفتن ریسک‌ها و هزینه‌های ناشی از پیاده شدن غلط و بی‌برنامه این نوع خدمات نشوند که در این صورت، باید هزینه‌ها و مخاطرات بسیاری را تحمل کنند. بر این اساس، هر گونه تصمیم‌گیری و اقدامی برای ارائه خدمات بانکداری الکترونیک اعم از اینترنتی، تلفن همراه، تلفن ثابت و غیره باید در چارچوب ساختار استراتژیک و سیاست‌های بلند مدت بانک و بدون شتابزدگی انجام بگیرد و تحلیل‌های هزینه در برابر درآمد و برآورد مخاطرات حتماً باید در این گونه اقدامات لحاظ شود.

امروزه، اینترنت و تلفن همراه باعث شده‌اند تا توانایی بانک‌ها و مؤسسات مالی برای عرضه محصولات و خدمات آنها در سر تا سر جهان افزایش چشمگیری یابد، با این همه، ریسک‌های حقوقی، اعتباری و قانونی بسیاری در اطراف بانکداری الکترونیکی برون مرزی، منطقه‌ای و بین‌المللی وجود دارد که بخش عمده این ریسک‌ها، ریشه در قوانین، سیاست‌ها و رویکردهای متفاوتی دارد که در بخش بانکداری الکترونیک، در کشورهای مختلف جهان وجود دارند. امروزه شاهد هستیم که الزامات کاملاً متفاوتی از نظر اعطای مجوز فعالیت بانکی آن لاین، نظارت بر این فعالیت‌ها و نحوه حمایت و حفاظت از مصرف کنندگان محصولات بانکی الکترونیک، در اقصی نقاط جهان وجود دارد که تعامل و تعاطف با آنها مستلزم صرف زمان و هزینه فروانی است. بر همین اساس، بانک‌ها باید پیش از هر گونه اقدام و تصمیم گیری برای راه اندازی بخش جدیدی برای ارائه خدمات بانکداری الکترونیکی، به ویژه در سطح منطقه‌ای و بین المللی، به ریسک‌ها و مخاطرات احتمالی آنها بیندیشند.

۲) کنترل‌های امنیتی:

در عهدنامه باسل ۲ و در بخش‌های مربوط به بانکداری الکترونیک آن، به یک سری فرایندهای کنترل امنیتی اشاره شده است که نیازمند دقت و توجه ویژه مدیریت بانک‌ها هستند و عامل اصلی متمایز کننده آنها از سایر فرایندهای کنترلی، متغیر و پیچیده بودن مسائل مرتبط با بانکداری الکترونیک و چالش‌های فراروی آن می‌باشد. در بخشی از مفاد عهدنامه باسل۲ آمده است: «الزامات مربوط به شناسایی و تأیید هویت مشتریان و کاربران خدمات بانکداری الکترونیک در مراحل مختلف استفاده از این خدمات، گامی اساسی و مهم برای کاهش ریسک‌هایی چون سرقت اطلاعات شخصی و شناسه‌ها محسوب می‌شود.»

روش های گوناگونی وجود دارند که با استفاده از آنها، بانک‌ها قادر خواهند بود با شناسایی درست و مطمئن کاربران خود، از پدیده‌هایی چون برداشت غیر قانونی از حساب افراد، پول شویی و هک شدن سیستم‌های بانکداری اینترنتی و تلفن همراه خود، جلوگیری کنند. بر این اساس، یک سری رمزهای عبور و کدهای دیجیتال، در زمان افتتاح حساب آن لاین یا تلفن همراه، در اختیار مشتریان متقاضی برخورداری از خدمات بانکداری الکترونیک قرار می‌گیرد که آنها را قادر می‌سازد تا هر زمان که می‌خواهند و فقط با وارد کردن این اطلاعات خاص، وارد سیستم شده و از خدمات موجود استفاده کنند.

بانک‌ها باید پیش از هر گونه اقدام و تصمیم‌گیری برای راه‌اندازی بخش جدیدی برای ارائه خدمات بانکداری الکترونیکی به ویژه در سطح منطقه‌ای و بین‌المللی، به ریسک‌ها و مخاطرات احتمالی آنها بیندیشند

بانک‌ها و مؤسسات مالی ارائه دهنده خدمات بانکداری الکترونیک، به سیستم‌های امنیتی و کنترلی خاصی نیاز دارند تا بتوانند مبدأ و فرستنده تقاضاهای نادرست و اغلب غیر قانونی و جعلی ورود به سیستم‌های آن لاین خود را شناسایی کنند و به بانک در پیگیری تخلف از طریق قانونی و قضایی یاری رسانند. بانک‌ها باید تمهیدات

ویژه‌ای را برای جلوگیری از افشای عمدی یا سهوی اطلاعات شخصی و مالی مشتریان آن لاین خود بیندیشند. لذا در زمان دریافت، ثبت وضبط داده‌های مربوط به این مشتریان، باید کلیه نکات و مسائل امنیتی را در نظر داشته باشند. در غیر این صورت، ضرر و زیان‌های اعتباری، مالی و حقوقی بسیاری دامنگیر بانک خواهد شد.

از سویی دیگر، هیأت مدیره بانک و مدیریت ارشد بانک‌های ارائه دهنده خدمات بانکداری الکترونیک باید در فواصل زمانی مشخص (مثلا هر ۶ ماه یا یک سال) نسبت به تطبیق سیستم‌های کنترلی خود (برای بانکداری الکترونیک) با استانداردهای بین المللی اقدام کنند و ممیزی‌ها و نظارت‌های دوره‌ای کامل و همه جانبه‌ای را در این مورد، اِعمال دارند.

در سال‌های اخیر، موارد متعددی از به سرقت رفتن اطلاعات محرمانه کاربران خدمات بانکداری همراه و اختلاس از طریق همراه، گزارش شده است که به علت رشد فزاینده این موارد، اعتماد عمومی به خدمات بانکداری همراه در برخی کشورها، به شدت کاهش یافته است

۳) مدیریت ریسک‌های حقوقی و اعتباری:

بانک‌ها و مؤسسات مالی ارائه دهنده خدمات بانکداری الکترونیکی موظف‌اند تا به کلیه شکایات و اعتراضات مشتریان خود در ارتباط با نحوه خدمات رسانی بانکی آن لاین و تلفن همراه پاسخ گویند و مسئولیت هرگونه افشای اطلاعات یا ارائه نکردن خدمات کامل و مناسب به آنها را به عهده بگیرند. بر اساس مفاد عهدنامه باسل ۲، کاربران و مشتریان خدمات بانکداری الکترونیک باید از همان مزایا و حقوقی بهره‌مند شوند که برای مشتریان عادی و دارندگان حساب‌های سنتی وجود دارد.

بانکداران باید بدانند که سطح انتظارات و توقعات از کیفیت و کمیت خدمات بانکی الکترونیکی، بسیار بالاست و لذا، بانک‌ها باید بهترین خدمات بانکی را در کوتاه‌ترین زمان ممکن و با بالاترین ضریب امنیتی، در اختیار مشتریان آن لاین و تلفن همراه خود قرار دهند ودر صورتی که در انجام دادن این وظیفه کوتاهی کنند، باید مسئولیت کلیه پیامدهای منفی از جمله تبعات حقوقی وقضایی آن را بپذیرند. به همین منظور بانک‌ها مکلف‌اند مکانیزم‌های مناسبی را برای حصول اطمینان از ارائه دائمی و شایسته خدمات بانکداری الکترونیکی، طراحی کنند تا از این طریق از شر ریسک‌های حقوقی و اعتباری متعددی که حیثیت و اعتبار آنها را تهدید می‌کنند، در امان باشند.

کلام آخر

بانکداری الکترونیک با تمام فراز و نشیب‌هایی که در مدت عمر کوتاه خود داشته است، افق‌های جدیدی را فراروی بانکداران، مدیران، سیاستگذاران و مشتریان بانک‌ها و مؤسسات مالی مترقی قرار داده است. خدمات بانکی الکترونیکی، خیلی زود در میان بانک‌ها و مشتریان رواج یافت و مقبولیت قابل توجهی پیدا کرد. امروزه کمتر بانکی در جهان وجود دارد که فاقد سیستم های ارائه خدمات بانکداری الکترونیکی، اعم از اینترنتی، همراه، ATM یا تلفن بانک باشد. با این همه، یک سری نقطه ضعف‌ها و نارسایی‌هایی در نحوه خدمات رسانی بانکی الکترونیکی به چشم می‌خورد که باید هر چه سریع‌تر رفع شود تا از میزان ریسک‌ها و مخاطرات موجود در این بخش تا حد زیادی کاسته شود. بانک‌ها و مؤسسات مالی باید از نگاه منفعت گرایانه به خدمات رسانی الکترونیک بپرهیزند و به آن به عنوان عاملی برای تکمیل و پربارتر کردن فرایند خدمات رسانی مالی و نوسازی ساز و کارهای بانکی و تکنولوژیکی خود بهره گیرند.

استقبال چشمگیر و غیر قابل باور مردم آفریقا و آسیا از خدمات بانکداری همراه، این واقعیت را به ما گوشزد می‌کند که بانکداری الکترونیک، به ویژه ارائه خدمات مالی از طریق تلفن‌های همراه، بهترین روش برای پوشش دادن به کسانی است که تاکنون از امکانات و خدمات بانکی محروم بوده‌اند و از طریق روش های سنتی، امکان ارائه خدمات مالی و بانکی به آنها وجود نداشته است.

همه این اهداف، تنها زمانی قابل دسترس است که دامنه تأثیر گذاری منفی و نامطلوب ریسک‌ها و مخاطرات موجود بر سر راه خدمات رسانی مالی الکترونیک - که کم هم نیستند - محدود شود و مدیریت و کنترل جامع و مطلوبی بر این ریسک‌ها، اِعمال شود.