مطالعات علوم کاربردی در مهندسی

دوره ۹، شماره ۲، تابستان ۱۴۰۲

صفحات ۵۷-۴۴

Online ISSN: ۲۴۷۶-۴۵۰۷

Print ISSN: ۲۵۳۸-۲۰۵۵

www.irijournals.com

بررسی تأثیر امنیت شبکه و مدیریت امنیت اطلاعات بر بهبود خدمات الکترونیکی با نقش میانجی اعتماد الکترونیکی درک شده (مطالعه موردی: بانک صادرات)

حسین رضایی

کارشناسی ارشد، گروه مدیریت فناوری اطلاعات، واحد صفاشهر ، دانشگاه آزاد اسلامی ، صفاشهر، ایران.

چکیده

این پژوهش با هدف بررسی تأثیر امنیت شبکه و مدیریت امنیت اطلاعات بر بهبود خدمات الکترونیکی با نقش میانجی اعتماد الکترونیکی درک شده انجام شده است. جامعه اماری آن مدیران و معاونین شعب مختلف بانک صادرات شیراز می باشد که تعداد ۲۱۸ نفر به عنوان نمونه اماری در نظر گرفته شدند. پژوهش حاضر از منظر هدف از نوع کاربردی بوده و نوع تحقیق توصیفی و در چارچوب اصول نظری می باشد. در تحقیق حاضر، اطلاعات اولیه و مطالب مربوط به بخش ادبیات پژوهش از روش کتابخانه ای گردآوری شده است و ابزار گردآوری داده ها پرسشنامه استاندارد است که از ۲۲ سؤال تشکیل شده است و ضریب آلفای کرونباخ ان ۸۰۴/. می باشد که نشان دهنده پایا بودن آن است. به منظور تجزیه و تحلیل داده ها از نرم افزار PLS استفاده شده است. بر اساس نتایج بدست آمده از تحلیل های صورت گرفته امنیت شبکه و مدیریت امنیت اطلاعات بر بهبود خدمات الکترونیکی تأثیر دارد. امنیت شبکه بر اعتماد الکترونیکی درک شده تأثیر معناداری دارد. همچنین مدیریت امنیت اطلاعات بر اعتماد الکترونیکی درک شده و بر بهبود خدمات الکترونیکی تأثیر دارد و در نهایت اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی تأثیر دارد.

واژه‌های کلیدی: . امنیت شبکه، مدیریت امنیت اطلاعات، خدمات الکترونیکی ، اعتماد الکترونیکی درک شده.

مقدمه

رشد فراگیر فناوری اطلاعات و ارتباطات، تأثیر بسیار زیادی بر صنعت بانکداری داشته است. ارائۀ خدمات بانکی به مشتریان یکی از جدیدترین این فناوری‌هاست. خدمات بانکی امروزه در اقتصاد جهانی رشد چشمگیری داشته است و بطور کلی اهمیت مشتری در بخش خدمات به مراتب بیشتر از محصولات می‌باشد و با پیشرفت بشر نیاز به خدمات بیش از پیش خواهد بود. بخش عمده از خدمات جهانی، خدمات بانکی می‌باشد. این صنعت در جهان بخش مهمی از خدمات را تشکیل می‌دهد. در حالی که خدمات بانکی در جهان رشد سریعی دارد و تحولات جهانی شدن در خدمات بانکی رو به افزایش است، کشورهای در حال توسعه از جمله ایران باید خود را برای تحولات سریع در ارتباط با خدمات بانکی آماده کنند. با توجه به اهمیت روز افزون جلب رضایت مشتریان برای سازمان‌ها، مدیریت ارتباطات اثربخش و کارا با مشتریان به مسئله‌ای اساسی و مهم برای سازمان‌ها و از جمله بانک‌های دولتی (به ویژه با ورود بخش خصوصی) تبدیل گردیده است (گومز-کروز[1] ۲۰۱۹).

خدمات الکترونیکی فرصت منحصر به فردی را برای کسب و کارها فراهم می کند تا مدل های جدیدی را برای طراحی راهبردهای خدمات و توسعۀ خدمات جدید ارائه دهند. کیفیت خدمات الکترونیکی می تواند همان ارزیابی و قضاوت کلی مشتریان از برتری و کیفیت خدمات الکترونیکی عرضه شده در بازار مجازی تعریف شود. این تعریف با تعریفات کیفیت خدمات سازگار است (لیونیلا[2]و همکاران، ۲۰۲۰). خدمات الکترونیکی بانک در کشور به سرعت رو به رشد و گسترش است. با توجه به استفادۀ گسترده از موبایل و در دسترس بودن آن، تمایل بسیاری به استفاده از این دستگاه در انجام امور بانکی به خصوص در قشر جوانان و افراد تحصیلکرده وجود دارد. بانکداری مبتنی بر خدمات الکترونیکی یکی از جدیدترین دستاوردهای عرصه فناوری در صنعت بانکداری به شمار می‌رود و مزایای زیادی برای بانک‌ها و مشتریان آن‌ها فراهم نموده است. باقی ماندن در فضای رقابتی، کاهش هزینه، امکان فعالیت‌های ارتباطی گسترده‌تر، صرفه‌جویی در زمان و هزینه، امکان دسترسی آسانتر و در عین حال سرعت بالاتر ارائه خدمات را می‌توان مزایایی دانست که بانکداری مبتنی بر موبایل برای مشتریان بانک‌ها به ارمغان آورده است (رزمی و طالبی، ۱۳۹۸).

در ابتدا که ارائه خدمات الکترونیکی جایگزین خدمات سنتی گردید، ارتباط بین شبکه ها بدون در نظر گرفتن مسائل امنیتی طراحی شدند، لذا علیرغم منافعی که پیشرفت تکنولوژی برای بشر در برداشته، در معرض تهدید و سوء استفاده نیز بوده است. جهت جلوگیری از این خطرها مبحث امنیت مطرح می گردد که عامل موثری جهت پذیرش و استفاده بیشتر افراد از خدمات الکترونیکی می باشد. امنیت به طور عمومی شامل دور نگهداشتن افراد غیر مجاز از دسترسی به اطلاعات و اجازه دادن به افراد مجاز جهت دسترسی به دارایی های با ارزش می باشد. اکثر فعالیت های تجاری با اطلاعات شخصی و حساس مشتریان و خریداران درگیر هستند، پس امنیت این اطلاعات از ارزش زیادی برخوردار است. امنیت شبکه مهمترین و اصلی ترین نگرانی کاربران و حتی مدیران می باشد. در این خصوص زمانی که کاربران یک سیستم الکترونیک به شبکه اینترنت وصل می شوند تا از خدمات آنلاین استفاده کنند، اطمینان به سیستم از اهمیت فوق العاده ای برخوردار است و این اطمینان در صورتی بوجود می آید که شخصی باور کند که سازمان برای او شرایط و شاخص های مفید و مورد نیاز جهت انجام یک تراکنش موفق را فراهم آورده است (شیخان و آزادی، ۱۴۰۰).

[1] Gómez-Cruz

[2] Lionello

در روزگار جهانی شدن که در آن فناوری های الکترونیکی واسطه مرتبط کننده بین عوامل ارتباطی (افراد یا سیستم ها) می باشند، اهمیت اعتماد حتی بارزتر است. اعتماد در دریافت خدمات به صورت الکترونیکی به دلیل وجود عدم قطعیت ها و ریسک های ناشی از استفاده از فناوری، حفظ اطلاعات مالی، شخصی و معاملاتی افراد بسیار دارای اهمیت است. اعتماد در فضای مجازی نیز مانند اعتماد در محیط واقعی مفهومی ذهنی است، سطح اعتماد مورد نیاز برای ایجاد تراکنش با توجه به ویژگی های شخصی هر فرد متفاوت است، همچنین انسان ها طرز تلقی های متفاوتی نسبت به فناوری دارند (بن منصور[3] ۲۰۱۶).

اعتماد یک حالت روانشناختی است که طرفین معامله نسبت به تداوم رابطه تجاری خود و یا در رسیدن به هدفی که از پیش تعیین شده است، دارند. وقتی افراد در یک معامله به یکدیگر اعتماد می کنند، بدان معناست که آن ها وعده هایی را که داده اند در طول رابطه تجاری خود حفظ خواهند کرد. لازم است هر یک از طرفین معامله، در تجارت خود کمی ریسک کنند. مطالعه های انجام شده نشان می دهد که اعتماد به عنوان یکی از پیامدهای مهم کیفیت خدمات الکترونیکی هستند، که با رشد و گسترش تجارت الکترونکی اهمیت بیشتری پیدا کرده است (وستا و جلیلوند[4] ۲۰۲۲). علت اصلی عدم تمایل مشتریان به استفاده از خدمات الکترونیکی به مسایلی مانند حفظ حریم شخصی افراد و اعتماد به بانک مورد استفاده بستگی دارد؛ بنابراین تحقیق و بررسی بر نقش اعتماد آنلاین در ارتقای سطح جذب مشتریان در بانکداری الکترونیکی بسیار ضروری می باشد (اسلامی و همکاران، ۱۳۹۷).

مردم در قالب افتتاح انواع حساب بانکی، نگهداری نقدینگی خود را به بانک ها سپرده اند. بانک ها نیز به عنوان امین مردم وظیفه دارند که سازوکارهای کنترلی و حفاظتی دقیقی را اجرا کنند تا پرداخت پول صرفاً به شخص مورد نظرِ صاحب حساب انجام شود. برداشت پول از حساب های سنتی مستلزم حضور ذینفع و احراز هویت او توسط متصدی بانکی است؛ بنابراین اگر شخصی قصد کلاهبرداری از حساب بانکی دیگری را داشته باشد، باید به صورت متقلبانه اقدام به تحصیل ابزار برداشت نماید یا ابزار برداشت فیزیکی را جعل کند و چون بانک تا زمانی که احراز هویت نکند پولی پرداخت نخواهد کرد. اما برداشت پول در بانکداری آنلاین که یکی از کاربردهای فناوری اطلاعات است، متفاوت بوده و ابزار برداشت فیزیکی به گذر واژه و کارت بانکی، تغییر ماهیت داده است (امیری دوماری، ۱۳۹۹).

در این روش از بانکداری، احراز هویت توسط تجهیزات رایانه ای مثل دستگاه های خودپرداز یا کارت خوان های فروشگاهی انجام می شود؛ بنابراین گذر واژه یا رمز عبورِ عددی و کارت بانکی، جایگزین چک، دفترچهٔ حساب و گواهی سپرده شده است. استفاده از این ابزارها در درگاه های بانکی به منزلهٔ تصدیق هویت و مجاز بودن استفاده از آ نهاست و استفادهٔ غیر مجاز از این ابزارها همان سرقت هویت است و چون از این ابزارها برای تبادلات مالی یا انتقال و جابه جایی پول الکترونیکی استفاده می شود، به سوژه و هدف کلاهبرداران تبدیل شده است (ساپاتی[5] ۲۰۱۹)، از این رو مقوله امنیت شبکه دارای اهمیت بسیار زیادی است.

امروزه نقش حساس اطلاعات به عنوان یک سرمایه ارزشمند در سازمان، بر کسی پوشیده نیست. هرچه میزان بهره مندی سازمان ها از سیستم های اطلاعاتی پیشرفته بیشتر باشد، اهمیت موضوع مدیریت امنیت اطلاعات به عنوان یکی از ارکان مهم بقایای سازمان، بیش از پیش مشخص می گردد. اهمیت این مسئله در سازمان های مختلف، دارای حساسیت های متفاوتی

[3] Ben Mansour
[4] Vosta & Jalilvand
[5] Sapaty

است و مشکلات و موانع امنیتی، یکی از اساسی ترین موضوعات مطرح در زمینه سیستم های اطلاعاتی است. سیستم مدیریت امنیت اطلاعات، به عنوان ابزاری در راستای ارتقای امنیت اطلاعات و نیز ارتقای کاربرد سیستم های اطلاعاتی در سازمان مطرح است. این سیستم ها در واقع، مجموعه ای از سیاست ها، اهداف، راهبردها، دارائی های سخت افزاری و نرم افزاری، روش های امنیتی، مستندات، دستورالعمل های فنی و سیستمی، منابع انسانی، شناسایی و ارزیابی مخاطرات، کنترل امنیت شبکه و اطلاعات مطرح هستند که متناسب با زمینه کاری سازمان طراحی و پیاده سازی شده و وظیفه تداوم امنیت اطلاعات در سازمان را به عهده دارند (سلطانی میرزائی و منشی زاده نائین، 1399).

بسیاری از شکست های مربوط به پیاده سازی و به کارگیری سیستم های مدیریت امنیت اطلاعات در سازمان ها، ریشه در مشکلات سازمانی، عدم توجه کافی به موانع و چالش های مرتبط با وضعیت آمادگی سازمان قبل از پیاده سازی و انتخاب مدل مناسب پیاده سازی دارد. انتخاب استاندارد و مدل مناسب، یکی از چالش های بزرگ در پیاده سازی امنیت اطلاعات سازمان ها مطرح است (فنگ[6] و همکاران، ۲۰۲۰).

اطلاعات یکی از مهمترین سرمایه های بانک ها و موسسات مالی است حفاظت از اطلاعات برای ایجاد و حفظ اعتماد بین بانک و مشتریان آن ضروری است. اطلاعات به موقع و معتبر برای اجرای معاملات و پشتیبانی از موسسه مالی و تصمیمات مشتری لازم است. چنانچه اطلاعات برای طرفین غیرمجاز فاش شده و تغییر داده شوند یا در صورت نیاز در دسترس نباشند درآمدها و سرمایه یک بانک می توانند بطور زیادی تحت تاثیر واقع شوند. دستیابی به امنیت اطلاعات در بانک ها بدون جاری سازی سیستم مدیریتی امنیت اطلاعات مناسب مقدور نمی باشد. طراحی مدل مدیریت امنیت اطلاعات بر اساس ساختار، روش ها و فرایندهای بانک، فعالیتی است که از طریق آن می توان سه مفهوم خاص محرمانه بودن اطلاعات، صحت اطلاعات و در دسترس بودن اطلاعات را تضمین کرد که این عوامل منجر به ایجاد اعتماد الکترونیکی در میان مشتریان بانک می شود (آزادباد، ۱۴۰۰).

این پژوهش قصد دارد با بررسی هر یک از این متغیرها به بررسی تأثیر امنیت شبکه و مدیریت امنیت اطلاعات بر بهبود خدمات الکترونیکی بپردازد همچنین میزان تأثیر این دو متغیر (امنیت شبکه و مدیریت امنیت اطلاعات) را با نقش میانجی اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی در شعب بانک صادرات بسنجد.

بسط فرضیات و ارائه مدل مفهومی پژوهش

امنیت شبکه به مجموعه ای از سیاست ها، مقررات و تمهیداتی گفته می شود که توسط مدیر به منظور جلوگیری و نظارت بر دسترسی غیرمجاز، سواستفاده، اصلاح، جلوگیری از تغییرات و یا محدود کردن دسترسی، در شبکه های کامپیوتری و منابع قابل دسترسی در شبکه تدوین شده و به آن اعمال می گردد (کریم خانی و همکاران، ۱۳۹۲) و امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن دسترسی غیرمجاز به آنها اشاره می کند. طی سال های اخیر تهدیدات امنیتی فراوانی بر اطلاعات سازمان ها وارد آمده، سبب گشته تا آنها هزینه های گزافی را متحمل شوند، این مساله در مورد سازمان هایی که از سامانه های اطلاعاتی و اینترنتی تحت شبکه استفاده می کنند از اهمیت بیشتری برخوردار است، این امر مدیران عالی سازمان ها را بر آن داشته است تا نظام امنیتی ای را پیاده سازی نمایند تا این هزینه ها ر ا به حداقل برسانند (ماسریک[7] و همکاران، ۲۰۲۰).

[6] Feng

[7] Masrek

در این پژوهش دو متغیر امنیت شبکه و مدیریت امنیت اطلاعات به عنوان متغیر مستقل در نظر گرفته شده اند که محقق قصد دارد میزان تأثیر این دو متغیر را بر خدمات الکترونیکی که متغیر وابسته در نظر گرفته شده است بسنجد، از این رو دو فرضیه در نظر گرفته شده است:

۱. امنیت شبکه بر بهبود خدمات الکترونیکی تأثیر معناداری دارد.
۲. مدیریت امنیت اطلاعات بر بهبود خدمات الکترونیکی تأثیر معناداری دارد.

اعتماد الکترونیکی به حالتی ذهنی اطلاق می شود که در آن فرد به دلیل اقدام به خرید و فروش به صورت الکترونیکی، در حالتی آسیب پذیر قرار می گیرد. در این حالت اولا فروشنده الکترونیکی را شایسته انجام معامله می داند و ثانیا رفتار فروشنده از نظر وی قابل پیش بینی است و در نهایت فرد اعتماد دارد که فروشنده در رفتار خود با وی، خیرخواهی پیشه کرده است. جلب اعتماد مشتریان بانک به عنوان یکی از فاکتورهای کلیدی و از عناصر اصلی موفقیت در بانکداری الکترونیک محسوب می شود. بسیاری از مطالعات نشان می دهند که اعتماد از جنبه های مهم و ضروری در پذیرش بانکداری الکترونیکی و عنصر اساسی برای ایجاد روابط بلند مدت مشتریان با بانک می باشد (چیو[8] و همکاران، ۲۰۱۷).

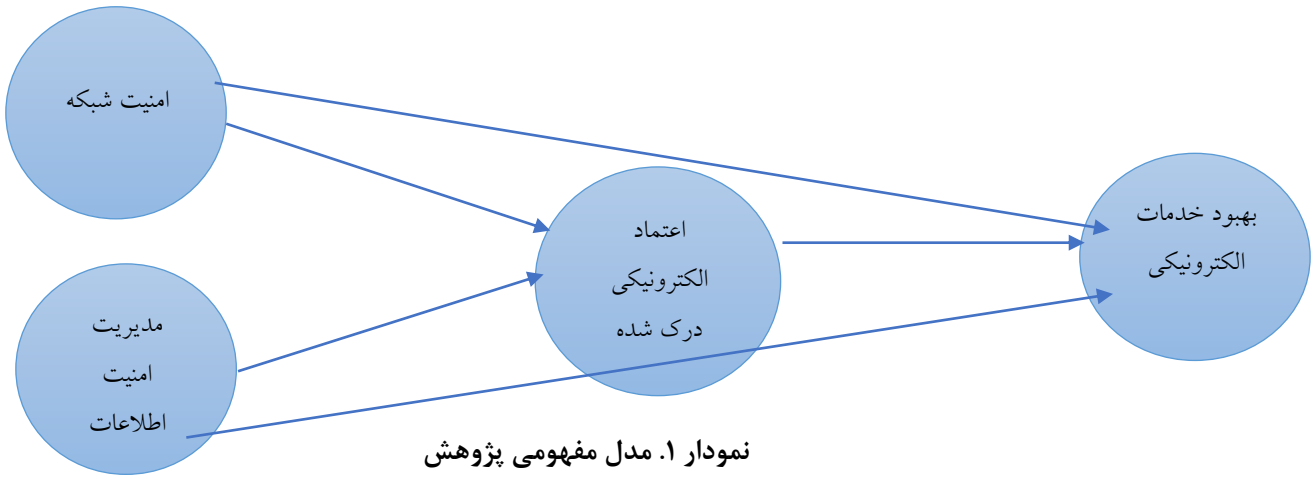
پژوهشگر قصد دارد با استفاده از دو فرضیه زیر نقش متغیر میانجی اعتماد الکترونیکی درک شده را نیز در رابطه میان دو متغیر مستقل و متغیر وابسته بسنجد.

۳. امنیت شبکه با نقش میانجی اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی تأثیر دارد.
٤. مدیریت امنیت اطلاعات با نقش میانجی اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی تأثیر دارد.

در ادامه پژوهشگر دو فرضیه دیگر در نظر گرفته است تا میزان تأثیر دو متغیر مستقل را به صورت جداگانه بر متغیر میانجی بسنجد و در نهایت محقق میزان تأثیر اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی را نیز می سنجد.

۵. امنیت شبکه بر اعتماد الکترونیکی درک شده تأثیر معناداری دارد.
٦. مدیریت امنیت اطلاعات بر اعتماد الکترونیکی درک شده تأثیر معناداری دارد.
۷. اعتماد الکترونیکی درک شده بر بهبود خدمات الکترونیکی تأثیر معناداری دارد.

که تمامی این فرضیات در قالب مدل مفهومی زیر ارائه شده است.



نمودار ۱. مدل مفهومی پژوهش

[8] Chiu

روش شناسی پژوهش

پژوهش حاضر از منظر هدف از نوع کاربردی بوده و نوع تحقیق توصیفی و در چارچوب اصول نظری می باشد. تحقیقات توصیفی با چگونگی و چرایی امور سروکار دارد و دامنه گسترده‌ای دارند و شامل مجموعه روش هایی است که هدف آن ها توصیف کردن شرایط یا پدیده های مورد بررسی است (حافظ نیا، ۱۳۸۷). تحقیقات کاربردی تحقیقاتی هستند که با استفاده از اطلاعات بدست آمده از تحقیقات بنیادی به پاسخ دهی مشکلات یا معضل های اجتماعی یا انسانی می پردازند. هدف از این تحقیقات، توسعه دانش کاربردی در یک زمینه خاص است (سرمد، ۱۳۹۰). جامعه اماری این پژوهش مدیران و معاونین شعب مختلف بانک صادرات شیراز می باشد که تعداد ۲۱۸ نفر به عنوان نمونه اماری در نظر گرفته شدند. در تحقیق حاضر، اطلاعات اولیه و مطالب مربوط به بخش ادبیات پژوهش از روش کتابخانه ای گردآوری شده است و ابزار گردآوری داده ها پرسشنامه استاندارد است که از ۲۲ سؤال تشکیل شده است و ضریب آلفای کرونباخ ان ۸۰۴/. می باشد که نشان دهنده پایا بودن آن است. همانطور که در بخش قبل توضیح داده شد برای این پژوهش ۷ فرضیه در نظر گرفته شده است که به منظور تجزیه و تحلیل داده ها و تأیید یا رد فرضیات از نرم افزار PLS استفاده خواهد شد

یافته های پژوهش

۱. آزمون نرمال بودن

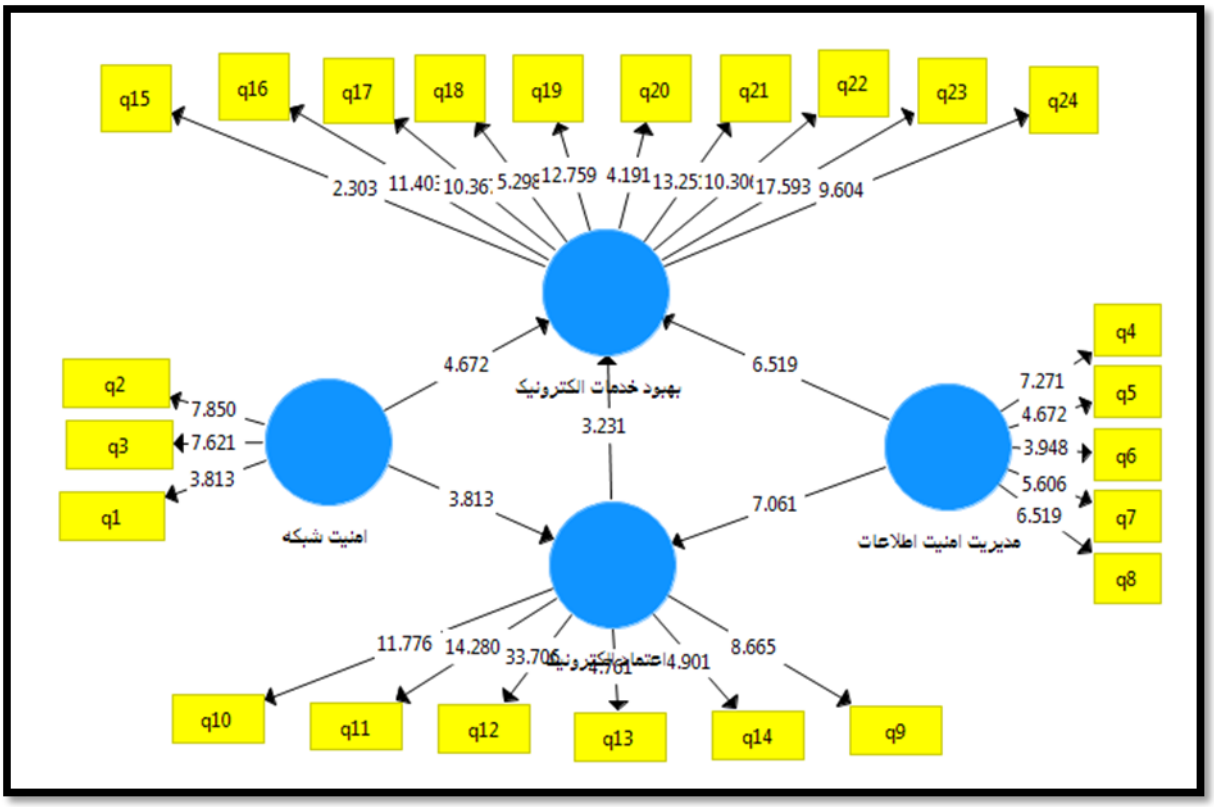
جهت تجزیه و تحلیل داده‌ها و انتخاب نوع آزمون‌های مربوطه، ابتدا باید به بررسی وضعیت نرمال بودن متغیرها بپردازیم. چرا که اگر متغیرها نرمال باشند، مجاز خواهیم بود هم از آزمون‌های پارامتریک و هم از آزمون‌های ناپارامتریک استفاده نماییم. اما چنانچه متغیرها نرمال نباشند، تنها مجاز خواهیم بود از آزمون‌های ناپارامتریک استفاده نماییم.نتایج نشان داد که فرض نرمال بودن با استفاده از ازمون کولموگوروف اسمیرنوف برای همه متغیرهای تحقیق رد می شود؛ چرا که سطح معنی داری آنها کوچکتر از ۰،۰۵ می‌باشد (جدول ۱). بنابراین از آزمون های ناپارامتریک استفاده خواهیم کرد.

جدول ۱. نتایج آزمون کولموگوروف اسمیرنوف برای بررسی فرض نرمال بودن

متغیرها	حجم نمونه	آماره آزمون	P-value
امنیت شبکه	۳۸۴	۴,۸۰۲	۰,۰۰۰
مدیریت امنیت اطلاعات	۳۸۴	۴,۴۳۱	۰,۰۰۰
اعتماد الکترونیک	۳۸۴	۴,۴۵۹	۰,۰۰۰
بهبود خدمات الکترونیک	۳۸۴	۵,۹۴۰	۰,۰۰۰

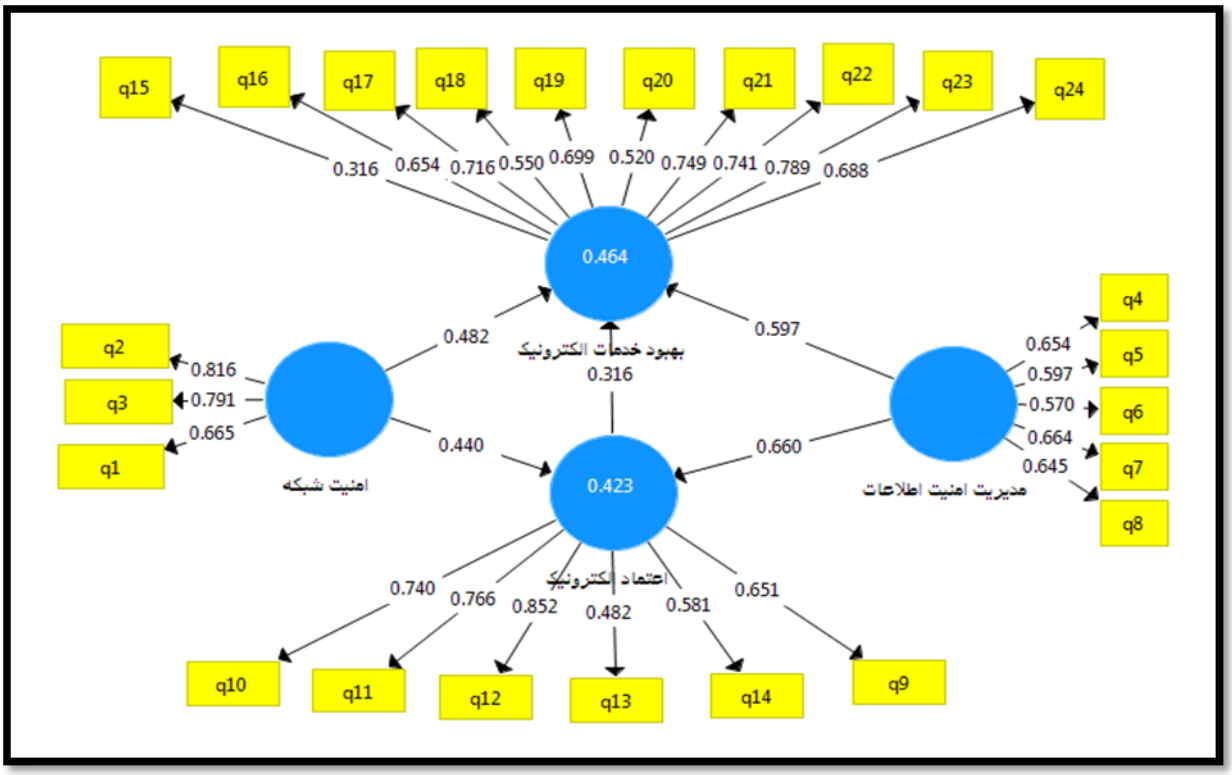
۲. نتایج تحلیل معادلات ساختاری (آزمون فرضیات)

پس از بررسی و تأیید الگو های اندازه گیری در گام اول، در گام دوم از معادلات ساختاری برای تست فرضیه ها استفاده شده است. برای آزمون معناری فرضیه ها از دو شاخص جزیی مقدار بحرانی و سطح معناداری استفاده شده است. مقدار بحرانی مقداری است که از حاصل تقسیم تخمین وزن رگرسیونی بر خطای استاندارد بدست می آید. براساس سطح معناداری ۰/۰۵، مقدار مسیر بحرانی باید بیشتر از ۱/۹۶ یا کمتر از ۱/۹۶- باشد و کمتر از این مقدار، پارامتر مربوط در الگو مهم شمرده نمی شود؛ و همچنین مقادیر کوچکتر از ۰/۰۵ برای مقدار سطح معناداری حاکی از تفاوت معنادار محاسبه شده برای وزن های رگرسیونی با مقدار صفر در سطح اطمینان ۰/۹۹ دارد.



شکل ۱. ضرایب معناداری t- value در حالت معناداری

دوره ۹، شماره ۲، تابستان ۱۴۰۲، صفحات ۵۷-۴۴



شکل ۲. ضریب مسیر در حال استاندارد

جدول ۲. نتایج اجرای الگویابی معادلات ساختاری فرضیه های پژوهش

روابط متغیرهای تحقیق	ارزش t	اثر مستقیم	اثرغیرمستقیم	سطح معناداری	نتیجه	رابطه
امنیت شبکه- بهبود خدمات الکترونیک	۴,۶۲	۰,۴۸	-	۰,۰۰۰	تایید	مستقیم
امنیت شبکه- اعتماد الکترونیک	۳,۸۱	۰,۴۴	-	۰,۰۰۰	تایید	مستقیم
مدیریت امنیت اطلاعات- بهبود خدمات	۶,۵۱	۰,۹	-	۰,۰۰۰	تایید	مستقیم
مدیریت امنیت اطلاعات- اعتماد	۷,۰۶۱	۰,۶۶	-	۰,۰۰۰	تایید	مستقیم
اعتماد الکترونیک- بهبود خدمات	۳,۲۳	۰,۳۱	-	۰,۰۰۰	تایید	مستقیم
امنیت شبکه- اعتماد الکترونیک- بهبود خدمات		-	۰,۴۴*۰,۳۱=۰,۱۳	-	تایید	مستقیم
مدیریت امنیت اطلاعات- اعتماد الکترونیک- بهبود خدمات الکترونیک		-	۰,۳۱*۰,۶۶=۰,۲۰	-	تایید	مستقیم

از آنجایی‌که در این تحقیق نقش میانجی‌گری متغیرها نیز بررسی می گردد، لازم به ذکر است که، در بررسی روابط میان متغیرها با وجود نقش متغیر میانجی بایستی اثرات مستقیم و غیر مستقیم مورد بررسی قرار گیرند. در صورتی که اثر غیر مستقیم بیشتر از اثر مستقیم باشد، نقش واسطه‌ای متغیر میانجی پذیرفته می‌شود. چنانچه عدد معناداری به دست آمده از این

طریق بزرگتر از قدر مطلق ۱/۹۶ باشد فرض صفر رد و فرض مقابل صفر تائید می شود. خلاصه نتایج در جدول ۳. آورده شده است.

جدول ۳. نتایج آزمون سوبل

فرضیه	ضریب تخمین غیر استاندارد مسیر اول	ضریب تخمین استاندارد مسیر دوم	خطای استاندارد مربوط به مسیر اول	خطای استاندارد مربوط به مسیر دوم	Z	نتیجه
امنیت شبکه- اعتماد الکترونیک- بهبود خدمات الکترونیک	**۰,۴۴**	۰,۳۱	۰,۰۵۱	۰,۰۴۹	۷,۴۰	تایید
مدیریت امنیت اطلاعات- اعتماد الکترونیک- بهبود خدمات الکترونیک	**۰,۶۶**	۰,۳۱	۰,۰۳۵	۰,۰۴۳	۱۰,۰۳	تایید

برای تعیین مسیرهای غیر مستقیم (اثر واسطه ای متغیر اعتماد الکترونیک) از روش بوت استراپ در برنامه ماکروی پریچر و هیز(۲۰۰۸) برروی نرم افزارSpss23 استفاده شد. جدول ۴. نتایج بوت استراپ را برای مسیرهای غیر مستقیم الگو نشان می دهد.

جدول ۴. نتایج بوت استراپ برای مسیرهای غیر مستقیم

مسیر	داده	بوت	سوگیری	خطای استاندارد	حدپایین	حد بالا
امنیت شبکه- اعتماد الکترونیک- بهبود خدمات الکترونیک	۰,۰۹۹۸	۰,۱۰۱۳	۰,۰۰۱۵	۰,۰۳۶۹	۰,۰۳۰۹	۰,۱۷۳۷
مدیریت امنیت اطلاعات- اعتماد الکترونیک- بهبود خدمات الکترونیک	۰,۰۷۴۱	۰,۰۷۲۳	-۰,۰۰۱۸	۰,۰۱۸۰	۰,۰۴۷۴	۰,۱۱۹۰

- با توجه به جدول ۴. حد بالا و پایین فاصله اطمینان برای اعتماد الکترونیک به عنوان متغیر میانجی بین متغیرهای امنیت شبکه و بهبود خدمات الکترونیک، صفر را در بر نمی‌گیرد. سطح اطمینان این فاصله اطمینان ۰,۹۵ درصد و تعداد نمونه گیری مجدد بوت استراپ ۱۰۰۰ می باشد. با توجه به اینکه صفر بیرون از این فاصله قرار می‌گیرد، رابطه غیر مستقیم متغیرها معنی دار می باشد. علاوه برآن نتایج آزمون بوت استراپ نیز نشان داد که روابط غیر مستقیم

در سطح ۰,۰۰۱ معنی دار می باشد. بنابراین متغیر اعتماد الکترونیک در رابطه امنیت شبکه و بهبود خدمات الکترونیک به عنوان متغیر میانجی ایفای نقش می‌کند.

- با توجه به جدول ۴. حد بالا و پایین فاصله اطمینان برای اعتماد الکترونیک به عنوان متغیر میانجی بین متغیرهای مدیریت امنیت اطلاعات و بهبود خدمات الکترونیک، صفر را در بر نمی‌گیرد. سطح اطمینان این فاصله اطمینان ۰,۹۵ درصد و تعداد نمونه گیری مجدد بوت استراپ ۱۰۰۰ می باشد. با توجه به اینکه صفر بیرون از این فاصله قرار می‌گیرد، رابطه غیر مستقیم متغیرها معنی دار می باشد. علاوه برآن نتایج آزمون بوت استراپ نیز نشان داد که روابط غیر مستقیم در سطح ۰,۰۰۱ معنی دار می باشد. بنابراین متغیر اعتماد الکترونیک در رابطه مدیریت امنیت اطلاعات و بهبود خدمات الکترونیک به عنوان متغیر میانجی ایفای نقش می‌کند.

۳. ضریب تعیین R^2 (R Squars)

معیار R^2 میزان تاثیر یک متغیر برون‌زا بر یک متغیر درون‌زا را مشخص می کند.نکته ضروری این است که مقدار R^2 تنها برای سازه‌های وابسته (درون‌زا) مدل محاسبه می‌گردد و در مورد سازه‌های برون‌زا، مقدار این معیار صفر است. هر چه مقدار R^2 مربوط به سازه‌های درون‌زای یک مدل بیشتر باشد، نشان از برازش بهتر مدل است. چاین (۱۹۹۸) سه مقدار ۰/۱۹، ۰/۳۳ و ۰/۶۷ را به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی بودن برازش بخش ساختاری مدل به‌وسیله معیار R^2 در نظرمی‌گیرد.

جدول ۴- ۱۲ ضریب تعیین

متغیر وابسته	R^2	شدت
بهبود خدمات الکترونیک	۰,۴۶۴	متوسط
اعتماد الکترونیک	۰,۴۲۳	متوسط
میانگین	۰,۴۴۳	متوسط

۴. کیفیت پیش بینی کنندگی (Q^2)

این معیار قدرت پیش‌بینی مدل را مشخص می‌سازد. مدل‌هایی که دارای پرازش بخش ساختاری قابل قبول هستند، باید قابلیت پیش‌بینی شاخص‌های مربوط به سازه‌های درون‌زای مدل را داشته باشند. هنسلر[9] و همکاران (۲۰۰۹) سه مقدار ۰/۰۲، ۰/۱۵ و ۰/۳۵ را برای نشان دادن قدرت پیش‌بینی ضعیف، متوسط و قوی سازه یا سازه‌های برون‌زای مربوط به آن تعریف کرده‌اند. ذکر این نکته ضروری است که این مقدار تنها برای سازه‌های درون‌زای مدل که شاخص‌های آن‌ها از نوع انعکاسی می-باشد، محاسبه می‌گردد.

[9] Hensler

دوره ۹، شماره ۲، تابستان ۱۴۰۲، صفحات ۵۷-۴۴

جدول (۴-۱۳) کیفیت پیش بینی کنندگی (Q^2)

متغیر وابسته	Q^2	شدت
بهبود خدمات الکترونیک	۰,۲۰۳	متوسط
اعتماد الکترونیک	۰,۴۱۸	قوی
میانگین	۰,۳۱۰	قوی

۵. برازش مدل کلی (GOF)

سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ به‌عنوان مقادیر ضعیف، متوسط و قوی برای این معیار معرفی شده‌است.

$$GOF = \sqrt{\overline{Communality} \times \overline{R^2}}$$ مدل $$= \sqrt{0.310 \times 0.443} = 0.370$$

با توجه به نتایج فوق می‌توان گفت که مدل برازش قوی دارد.

نتیجه گیری و پیشنهادات

ضریب نفوذ استفاده از خدمات الکترونیک به دلیل سهولت استفاده بالاتر از هر فناوری دیگری است و این مسأله، بانکداری را به شکل انقلابی جهانی درآورده است که با همان سرعت وقوع در کشورهای پیشرفته، در کشورهای درحال توسعه نیز معمول شده است. مفید و مناسب بودن خدمات بانکداری الکترونیک می تواند علاوه بر رفع نیازهای روزمره مشتریان بانک ها، به آن ها کمک کند تا در هر لحظه و در هر مکانی که هستند از موقعیت حساب های بانک خود مطلع شده و یا در آن ها تغییراتی را ایجاد نمایند. این امر به نوبه خود می تواند باعث رضایتمندی مشتریان بانک ها شود زیرا بانکداری الکترونیک دسترسی مشتریان به حساب هایشان را بسیار سریع و سهل الوصول کرده است و موارد خدماتی که بانک ها با ارایه آن ها می توانند موجبات رضایتمندی مشتریان خود را فراهم نمایند را بسیار گسترش داده است.

ارائه خدمات بانکی به صورت الکترونیک یکی از جدیدترین دستاوردهای عرصه فناوری در صنعت بانکداری به‌شمار می‌رود و مزایای زیادی برای بانک‌ها و مشتریان آن‌ها فراهم نموده است. از این رو علاقه‌مندی مدیران بانکی به دانستن این موضوع که چه فاکتورها و عواملی باعث افزایش اعتماد الکترونیک مشتریان می شود، قابل توجیه است و موجب فراهم نمودن امکان برنامه‌ریزی مناسب‌تر جهت افزایش کاربران خدمات الکترونیک بانکی و بهره‌مندی سریع‌تر از مزایای این پدیده را برای بانک‌ها و نیز کاربران این خدمات فراهم می‌آورد. امروزه به واسطه گسترش نفوذ اینترنت در جامعه، افراد بسیاری به دنبال استفاده از خدمات مختلف و متنوع آنلاین هستند. یکی از این خدمات که مورد استقبال زیادی نیز قرار گرفته است، خدمات بانکداری الکترونیک است. در این خدمت، بانک ها برخی از خدمات پرداخت را از طریق وبسایت اختصاصی خود و یا اپلیکیشن اختصاصی بانک و یا اپلیکیشن های رابط به مشتریان ارائه می کنند. سرعت و قابل دسترس بودن این خدمات در تمامی روزها و در هر ساعت از شبانه روز باعث شده است تا مشتریان اقبال بیشتری به بهره گیری از خدمات آنلاین بانکی داشته باشند.

هرگونه بهبود در اعتماد مشتریان موجب بهبود در رضایت آنها می گردد. بانک می تواند با ارائه خدمات الکترونیکی با کیفیت، از طریق سیستم های الکترونیکی خود، رضایت مشتریان را جلب نموده و از این طریق بر تکرار تراکنش مالی آنها تأثیر بگذارد. در محیط مبتنی بر فناوری امروزی، به دلیل نگرانی مشتری درباره اطلاعات مربوط به حریم خصوصی، بانک ها باید در جستجوی راه هایی باشند تا بر این نگرانی ها غلبه نموده و مشتریان را ترغیب کنند که اطلاعاتی را که می تواند به ارائه خدمات بهتر به آنها کمک نماید را در اختیار بانک ها قرار دهند. نگرانی زیاد درباره حریم خصوصی بر انتخاب فرد از بین دو بانکی که دارای شرایط مساوی هستند، تأثیر می گذارد. هنگامی که هیچ حضور فیزیکی لازم نیست، تأمین کننده خدمات الکترونیکی هر بانکی می تواند باشد، پس بنابراین بدست آوردن اعتماد مشتری با تأکید بر حفظ حریم خصوصی، امنیت و اطمینان، اهمیت بیشتری می یابد. مشتری که نگرانی کافی درباره حریم خصوصی خود دارد بانکی را که دارای توانایی بالایی در حفظ و استفاده از اطلاعات وی برای ارائه خدمات شخصی شده دارد، انتخاب خواهد نمود و این به نوبه خود بر سودآوری بانک تأثیر خواهد گذاشت.

اما در این میانه، همزمان با پیشرفت های صورت گرفته در حوزه خدمات بانکداری الکترونیک، مخاطرات و تهدیدهای الکترونیکی نیز افزایش داشته است، از این رو مدیریت امنیت اطلاعات و ارتقای امنیت شبکه از اهمیت بالاتری برخوردار شده است و بانک ها و سرویس دهندگان خدمات مالی الکترونیک باید به صورت مداوم به دنبال راهکارهایی برای بالاتر بردن امنیت شبکه های اطلاعاتی خود به منظور حفاظت از حریم خصوصی کاربران و جلوگیری از سرقت های اینترنتی باشند. یکی از مهمترین موانعی که در استفاده بیشتر از خدمات بانکداری الکترونیک وجود دارد، ترس مشتریان از قرار گرفتن در معرض سوء استفاده و ضررهای مالی است. نفوذ سارقان به محیط کاربری متشریان بانکداری الکترونیک می تواند باعث وارد آمدن ضررهای سنگین مالی به مشتریان شود که گاهاً این سرقت ها قابل پیگیری و باز پس گیری دارایی از دست رفته نمی باشند. این شرایط باعث می شود تا مشتریان در شرایط عدم قطعیت قرار گیرند و تصمیم گیری برای ایشان در خصوص استفاده از خدمات آنلاین بانکی همراه با ریسک به نظر برسد. مشخص است که در چنان شرایطی تمایل مشتریان به استفاده از خدمات آنلاین بانکداری تحت تأثیر اخبار و اتفاقات منفی قرار گرفته و با اُفت قابل توجهی همراه خواهد بود. اما از سوی دیگر، مدیریت بهینه امنیت اطلاعات و استفاده از تجهیزات و نرم افزارهایی که امنیت شبکه را افزایش می دهند می تواند در بهبود روند فوق الذکر تأثیر قابل قبولی داشته باشد. همزمان با افزایش میزان سرقت های آنلاین، شرکت های تولید کننده نرم افزارها و سخت افزارهای امنیتی نیز به سرعت در حال تغییر هستند تا بتوانند به روزترین و ایمن ترین تجهیزات و نرم افزارها برای جلوگیری از سرقت های آنلاین را در اختیار بانک ها و دیگر ارائه دهندگان خدمات مالی آنلاین قرار دهند. استفاده از این تجهیزات و امکانات با عث افزایش امنیت و کاهش نفوذپذیری شبکه می شود. در ادامه پیشنهاداتی به مدیران شعب مختلف بانک صادرات در شیراز ارائه می گردد که به انها کمک می کند تا در جهت ارتقای سطح امنیت شبکه و مدیریت بهینه امنیت اطلاعات در راستای بالا بردن اعتماد الکترونیک درک شده مشتریان خود فعالیت نمایند:

- استفاده از سخت افزارهای محافظتی قوی تر که امکان ایجاد FireWall سخت افزاری برای سامانه را فراهم می سازند از جمله راهکارهایی که امروزه برای ارتقاء امنیت شکبه های خدمت رسان الکترونیک مورد استفاده قرار می گیرد.
- اطلاع رسانی به مشتریان در خصوص امکانات دفاعی و امنیتی ایجاد شده بر بستر سامانه بانکداری الکترونیک جهت افزایش اعتماد ایشان به استفاده از خدمات آنلاین.

- استفاده از تیم های حرفه ای برای پیگیری دقیق تر و عمیق تر حملاتی که به سامانه های بانکداری صورت می گیرد جهت شناسایی منبع حمله و در اختیار قرار دادن اطلاعات مربوطه به پلیس فتا.
- استفاده از روش های تشخیص هویت قدرتمندتر جهت اطمینان از عدم امکان ورود غیر مجاز به حساب کاربری مشتریان.
- استفاده از فناوری امنیتی SSL به منظور برقراری ارتباط امن بین کاربر و سرور ارائه دهنده خدمات الکترونیک.
- آگاهی به مشتریان در خصوص توجه به پروتکل Https در زمان ورود به هرگونه درگاه پرداخت اینترنتی جهت اطمینان در خصوص واقعی بودن درگاه.
- اجبار کابران به استفاده از گذرواژه های پیچیده که همزمان از حروف بزرگ و کوچک، اعداد و کاراکترهای غیر عددی و غیر حرفی تشکیل شده باشد جهت افزایش امنیت سامانه.
- اطلاع رسانی دقیق تر به مشتریان در خصوص عدم افشای اطلاعات هویتی و اطلاعات ورود به سامانه های بانکداری جهت جلوگیری از ضررهای مالی.
- برقراری امکانات اطلاع رسانی فوری در خصوص ورود به سامانه بانکداری مشتری توسط پیامک و اطلاع فوری ایشان.
- هم چنین مدیران بانک باید نسبت به تقویت زیرساخت های تکنولوژیکی (تکنیک های رمزنگاری و رمزگشایی، دیوارآتش، امضای دیجیتالی و....) بپردازند که این اقدام می تواند گام موثری را در جلب اعتماد آنلاین مشتریان در مبحث امنیت الکترونیکی بردارند.

منابع و مؤاخذ

۱. آزادباد، ه.، ۱۴۰۰. بررسی راهکارهای بهبود امنیت شبکه و پیشگیری از حملات امنیتی. *ششمین کنفرانس بین المللی مهندسی برق،کامپیوتر و مکانیک*، ۱۹۸-۱۸۷.

۲. اسلامی، ز.، رستم زاده، پ.، و آواساپیان، آ. (۱۳۹۷). بررسی عوامل موثر بر افزایش اعتماد مشتریان در خرید الکترونیکی. دومین همایش بین المللی مدیریت، حسابداری و اقتصاد در توسعه پایدار. مشهد: موسسه تعاونی دانش بنیان کمرآوش.

۳. امیری دوماری، س. (۱۳۹۹). مروری بر مدل های کسب و کار الکترونیکی. هفتمین کنگره ملی تازه یافته های مهندسی برق ایران، (ص. ۲۷۳-۲۸۶). تهران.

۴. حافظ نیا، م. (۱۳۸۷). *مقدمه ای بر روش تحقیق در علوم انسانی*. تهران: انتشارات سمت.

۵. رزمی، ع. و طالبی، ر.، ۱۳۹۸. میزان تاثیر خدمات بانکداری الکترونیکی در افزایش منابع و درآمدهای کارمزدی (مطالعه موردی: پایانه های فروش بانک کشاورزی استان مرکزی)، کنفرانس جهان الکترونیک، تهران، موسسه آموزشی عالی مهر اروند و مرکز راهکارهای دستیابی به توسعه پایدار.

۶. سرمد، ز.، بازرگان، ع. و حجازی، ا.، ۱۳۹۰. روش های تحقیق در علوم رفتاری. تهران: انتشارات نشر آگه.

۷. سلطانی میرزائی، م. و منشی زاده نائین، ح.، ۱۳۹۹. تشخیص سرقت های آنلاین در شبکه اینترنت و شبکه های اجتماعی با شبکه عصبی مصنوعی چند لایه و انتخاب ویژگی. *چهارمین کنفرانس بین المللی تحقیقات بین رشته ای در مهندسی برق، کامپیوتر، مکانیک و مکاترونیک در ایران و جهان اسلام*، ۳۲۷-۳۱۲.

۸. شیخان، م. و آزادی، ک.، ۱۴۰۰. یک چارچوب بهبودیافته برای بهبود کیفیت و امنیت در شبکه اینترنت اشیاء با استفاده از زنجیره بلوکی و قدرت پردازشی لایه مه. *فناوری اطلاعات و ارتباطات ایران*، جلد ۱۳(۴۸-۴۷)، ۱۱-۲۲.

۹. کریم خانی، ف.، عسگر اقدم، ه. و احمدی رند، ط.، ۱۳۹۲. *پردازش ابری: امنیت شبکه در بانکداری الکترونیک. کنفرانش مقابله با چالش های امنیت شبکه*، شوشتر، رویکرد جهانی مدیران، ۱ (۳)، ۱۵۸-۱۴۲.

10. Ben Mansour, K. (2016). An analysis of business' acceptance of internet banking: an integration of e-trust to the TAM", ,. *Journal of Business & Industrial Marketing, Vol. 31 No. 8*, 982-994.

11. Chiu, J. L., Bool, N. C., & Chiu , C. L. (2017). Challenges and factors influencing initial trust and behavioral intention to use mobile banking services in the Philippines. Asia Pacific Journal of Innovation and Entrepreneurship, 11(2), 246-278.

12. Feng, W., Wu, Y. & Fan, Y., 2020. A new method for the prediction of network security situations based on recurrent neural network with gated recurrent unit. *International Journal of Intelligent Computing and Cybernetics*, Volume Vol. 13 No. 1,, 25-39.

13. Gómez-Cruz, M., 2019. Electronic reference services: a quality and satisfaction evaluation. *Reference Services Review*, Volume Vol. 47 No. 2, 118-133.

14. Lionello, R., Slongo, . L. & Matos, C., 2020. Electronic service quality: a meta-analysis. *Marketing Intelligence & Planning*, Volume Vol. 38 No. 5, 619-635..

15. Masrek, M., Sani, A. & Zaini, M., 2020. The impact of information security management practices on organisational agility. Information and Computer Security, Volume Vol. 28 No. 5, 681-700.

16. Sapaty, P., 2019. Networked Security Related Solutions", Complexity in International Security. *Emerald Publishing Limited, Bingley*, 79-92.

17. Vosta, L., & Jalilvand, M. (۲۰۲۲). Electronic trust-building for hotel websites: a social exchange theory perspective. Journal of Islamic Marketing, ۳(۷), ۵۸۲-۵۶۳.