

Paper Type: Original Article



The Effect of Applying Protective Measures Against Identity Theft on Online Purchase Intention (Sobel Mediation Analysis Approach)

Mostafa Heidari Haratemeh^{1,*} , Farzad Torabi²

¹ Department of Economics, Naraq Branch, Islamic Azad University, Naraq, Iran; heidarimu@yahoo.com.

² Department of Business Administration, Narag Branch, Islamic Azad University, Narag, Iran; farzad_1974@yahoo.com.

Citation:



Heidari Haratemeh, M., & Torabi, F. (2025). The effect of applying protective measures against identity theft on online purchase intention (Sobel mediation analysis approach). *Innovation management and operational strategies*, 6(1), 112-127.

Received: 09/08/2024

Reviewed: 13/11/2024

Revised: 25/12/2024

Accepted: 19/01/2025

Abstract

Purpose: The purpose of this research is to investigate the integrated effect of applying protective measures against identity theft on consumers' synergistic perception of trust, cost of products/services, and operational performance on online purchase intention.

Methodology: To collect data, a 41-item standard questionnaire with a Likert scale was used. To know the works of structures from the model (IT-OPI) [1] have been used. Through a short interview with 650 students, 242 students who make online purchases once a month were selected, and finally, 200 people were considered as samples according to their previous experience in shopping and frequency of interaction with different websites.

Findings: In e-commerce, operational performance and trust have a potential effect on the pursuit of consumer purchase intention. Traditionally, price is always an issue in marketing. However, for e-commerce, this does not have a direct impact on the purchase intention. The overall joint effect of operational performance, trust and price on purchase intention is neither negative nor neutral. Synergistically, the use of identity theft control tools can significantly increase consumer trust, which is the only predictor for pursuing consumer purchase intention.

Originality/Value: If consumers find the use of control mechanisms against cybercrime, especially identity theft, to increase the reliability, validity and security of transactions online, paying more is less important to them. Because creating trust in buying is not the price but the driving force.

Keywords: Perceived trust, E-commerce, Identity theft, Operational performance, Purchase intention.



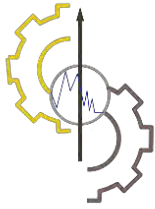
Corresponding Author: heidarimu@yahoo.com



10.22105/imos.2024.462044.1361



Licensee. **Innovation Management & Operational Strategies**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).



تاثیر اعمال اقدامات حفاظتی در برابر سرقت هویت بر قصد خرید آنلاین (رویکرد تحلیل میانجی سوبل)

مصطفی حیدری هراتمه^{۱*}، فرزاد ترابی^۲

^۱گروه اقتصاد، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران.

^۲گروه مدیریت بازرگانی، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران.

چکیده

هدف: هدف تحقیق حاضر، بررسی تاثیر یکپارچه اعمال اقدامات حفاظتی در برابر سرقت هویت بر درک هم افزایی مصرف کنندگان از اعتماد، هزینه محصولات/خدمات و عملکرد عملیاتی بر قصد خرید آنلاین است.

روش شناسی پژوهش: جهت جمع آوری داده ها، از پرسشنامه استاندارد ۴۱ گویه ای با مقیاس لیکرت استفاده شد. برای شناخت آثار سازه ها از مدل [1] (IT-OPI) استفاده شده است. از طریق یک مصاحبه کوتاه با ۶۵۰ دانشجوی ۲۴۲ دانشجو که ماهی یک خرید آنلاین دارند انتخاب و نهایتاً ۲۰۰ نفر با توجه به تجربه قبلی آن ها در خرید و تناوب تعامل با وبسایت های مختلف به عنوان نمونه در نظر گرفته شد.

یافته ها: در تجارت الکترونیک، عملکرد عملیاتی و اعتماد تاثیر بالقوه ای بر پیگیری قصد خرید مصرف کنندگان دارد. به طور سنتی، قیمت همیشه یک موضوع در بازاریابی است. اما برای تجارت الکترونیک این موضوع تاثیر مستقیمی بر قصد خرید ندارد. تاثیر مشترک کلی عملکرد عملیاتی، اعتماد و قیمت بر قصد خرید نه منفی است و نه خنثی. به صورت هم افزایی، استفاده از ابزارهای کنترل کننده سرقت هویت می تواند به طور قابل ملاحظه ای اعتماد مصرف کنندگان را افزایش دهد، که تنها پیش بینی کننده برای پیگیری قصد خرید مصرف کننده است.

اصالت/ارزش افزوده علمی: اگر مصرف کنندگان کاربرد مکانیسم های کنترلی در برابر جرایم سایبری، به ویژه سرقت هویت، افزایش قابلیت اطمینان، اعتبار و امنیت تراکنش ها را در فضای آنلاینی پیدا کنند، پرداخت مبلغ بیشتر برایشان اهمیت کمتری دارد. زیرا ایجاد اعتماد در خرید، قیمت نیست بلکه نیروی پیشران و محرکه است.

کلیدواژه ها: اعتماد درک شده، تجارت الکترونیکی، سرقت هویت، عملکرد عملیاتی، قصد خرید.

۱- مقدمه

با توجه شیوه های تجارت مبتنی بر یک محیط تجارت الکترونیکی با توجه به سرعت و توسعه روزافزون فناوری اطلاعات و ارتباطات، به ویژه فناوری گوشی های همراه، به سرعت در حال گسترش هستند. با توجه به تغییر سبک زندگی، شهرنشینی، زیست شهری و استفاده زیاد و عادت به فناوری و مهم تر در شرایط ضروری همچون تجربه کووید، مصرف کنندگان به طور فزاینده ای به استفاده از دولت الکترونیک، محیط تجارت الکترونیکی و رسانه های اجتماعی مبتنی بر برنامه ها و سایت هایی برای تسهیل فعالیت های خرید معمول و تعامل با آن ها علاقه مند هستند [2-6]. استفاده و عادت روزافزون مصرف کنندگان به خرید آنلاین باعث ایجاد پنجره جدیدی برای بازاریابان برای تبلیغ و فروش مستقیم محصولات خود به مشتریان است. از سوی دیگر، به طور مداوم، تهدیدها و نقص های امنیتی متعدد و جدیدی مرتبط با فناوری و خطرات بالقوه آن وجود دارد. یعنی جرایم سایبری به سرعت با نرخ تصاعدی در حال افزایش است [7].

مطالعات اولیه در مورد این موضوع نشان داده است [8] که از اشکال متعدد جرایم سایبری، سرقت هویت یکی از مهم‌ترین مسایل برای مدیریت یک محیط تجارت الکترونیکی است. سرقت هویت به‌عنوان مانعی بزرگ در برابر گسترش بیشتر خریدهای آنلاین در کانال‌های در حال ظهور عمل می‌کند [9]. این موضوع مهم زمینه را برای انجام تحقیقات بیشتر جهت درک مسایل مربوط به آن و تدوین توصیه‌های مرتبط که می‌تواند به یک محیط تجارت الکترونیکی کمک کند، فراهم می‌کند. تا از این طریق خرده‌فروشان تأثیر چنین چالش‌هایی را به حداقل برسانند. تحقیقات گذشته به مسایل مربوط به یک محیط تجارت الکترونیکی کمک کرده‌اند که شامل مسایلی مانند خطرات در معاملات یک محیط تجارت الکترونیکی [1]، [3]، [10]، نگرش اعتماد مصرف‌کنندگان در خرید از یک محیط تجارت الکترونیکی [11]، رفتار خرید مصرف‌کنندگان و معیارهای پذیرش یک رسانه مجازی به‌عنوان یک کانال بازاریابی [2]، [12] و جرایم سایبری [7] می‌باشد. این مطالعات تهدیدات بالقوه در رسانه مجازی و حفره‌های امنیتی آن را بررسی کرده‌اند [3]، [9]؛ همچنین مطالعات موجود تأثیر گسترده ظهور تهدیدات امنیتی و نحوه مدیریت آن‌ها را بررسی کرده و توصیه‌هایی برای به حداقل رساندن آثار مخرب آن ارائه داده‌اند. مطالعات مرتبط با رفتار فناوری، محیط تجارت الکترونیکی، دولت الکترونیک، بانکداری تلفن همراه و سلامت آن [13-15]، نشان دادند که چگونه گسترش فناوری می‌تواند زمینه‌های سرقت هویت و جرایم سایبری را ایجاد کند.

محققان بازاریابی و رفتار مصرف‌کننده [16]، نیز چنین موضوعاتی را بررسی کرده‌اند تا مانع گسترش بدون ضابطه رسانه‌های مجازی مانند محیط تجارت الکترونیکی شوند چراکه به‌خوبی تشخیص داده شده است که رشد مورد انتظار یک محیط تجارت الکترونیکی به‌شدت توسط بسیاری از انواع خطرات ناشی از چالش‌های نوظهور مانند سرقت هویت با مانع روبرو شده است، کند شده و به خطر می‌افتد [14]، [15]. از این رو، استدلال شده است که جرایم سایبری (مانند سرقت هویت) باید کنترل و به حداقل برسد تا از تأثیر منفی آن بر رشد و انتشار رسانه‌های خرید آنلاین/مجازی جلوگیری شود [13]. برای این منظور، ابتدا چارچوب نظری و پیشینه پژوهش به همراه تبیین و توسعه فرضیه‌های پژوهش ارائه می‌شود و در ادامه به روش‌شناسی تحقیق و زیر بخش‌های آن پرداخته و نهایتاً به نتیجه‌گیری به همراه مفاهیم نظری سیاستی پرداخته خواهد شد.

۲- چارچوب نظری تحقیق

در چارچوب مطالعات مرتبط با سرقت هویت، جرایم سایبری، اعمال اقدامات کنترلی و تأثیر آن بر قصد خرید در یک محیط تجارت الکترونیکی، با مفهوم‌سازی اولیه و کاربردی کردن آن، می‌توان مبانی نظری آن را توسعه و عملیاتی کرد. اقدامات عملیاتی و کاربردی برای محافظت/کنترل سرقت هویت متناسب با یک محیط تجارت الکترونیکی شامل قوانین جهانی، کنترل سازمان‌ها، مدیریت فنی، سیاست‌های مدیریتی، انتشارات برای توسعه آگاهی، ابزارهای مدیریت ریسک، مدیریت داده‌ها و کنترل بر کارکنان، بر اساس مطالعات موجود طراحی شده است [5]، [7]، [13].

این مطالعات در مورد عملکرد یک محیط تجارت الکترونیکی توصیه کرده‌اند که کاربرد و پیاده‌سازی اقدامات کنترلی در چنین محیطی به‌شدت آسیب‌پذیر بوده و نیاز است جهت بازدهی و عملکرد بیشتر و موثرتر موردتوجه و بررسی بیشتری قرار گیرد [13]، [14]، [17]، [18]. مطالعه حاضر در راستای نتایج مصاحبه‌ها با مدیران یک محیط تجارت الکترونیکی که برای کنترل سرقت هویت، تکنیک‌های مختلف حفاظتی دارند، مفروض و ترسیم شده است. طبیعی است که این اقدامات ممکن است آثار ترکیبی و هدایت‌کننده شدیدی بر هزینه محصولات/خدمات، عملکرد عملیاتی و داشته و ادراک مصرف‌کنندگان از اعتماد درحالی‌که قصد خرید در یک محیط تجارت الکترونیکی یا آنلاین را دارند، داشته باشند. هم محققین و هم مدیران در رابطه با یک محیط تجارت الکترونیکی احساس می‌کنند که تأثیر یکپارچه هزینه محصولات/خدمات، عملکرد عملیاتی و اعتماد مصرف‌کنندگان در وبسایت‌ها، تأثیر قابل توجه و معناداری بر قصد خرید مصرف‌کنندگان دارد [19]، [20]. از این رو در مورد جرایم سایبری و تأثیر مشترک آن بر قصد خرید توصیه به درک و فهم قصد خرید مصرف‌کنندگان هم‌زمان از طریق تأثیر یکپارچه هزینه محصولات/خدمات، عملکرد عملیاتی و اعتماد مصرف‌کنندگان در وبسایت‌های یک محیط تجارت الکترونیکی می‌کنند. در این مطالعه برای حمایت از مدل نظری و فرضیه‌های پیشنهادی، یک بررسی پیمایشی اکتشافی در بین مدیران محیط تجارت الکترونیکی انجام گرفت. جهت بررسی و تأیید اعتبار سه ساختار، سازه یا مولفه بالقوه شامل اعتماد درک شده، ارزش قیمت درک شده و عملکرد عملیاتی که برگرفته از بررسی ادبیات آن و مدل پیشگیری، از مطالعه شریف و کومار [21] در یک محیط تجارت الکترونیکی و تأثیر آن‌ها بر قصد خرید موردبررسی قرار گرفته است.

معاملات و تجارت بین تولیدکننده و مصرف‌کننده (B2C) یک محیط تجارت الکترونیکی یا آنلاینی از قرن گذشته آغاز و به وجود آمد و اکنون شتاب آن به میزان قابل توجهی از سوی مشتریان در حال افزایش است. این نوع از تجارت، مشتریان زیادی را برای خرید آنلاین جذب کرده است و با گنجاندن بیشتر مشتریان جدید و شرکت‌های جدید در حال گسترش است. مصاحبه‌ها با مدیران این حوزه با استفاده از یک پرسشنامه نیمه

ساختاریافته مربوط به سه سازه از پیش تعریف شده مدل منبع-پیشگیری (Source-Prevention Model) انجام شد. خروجی مصاحبه نشان داد که پس از اعمال بسیاری از ابزارهای کنترل سرقت هویت، تجارت در فضای آنلاین با چالش‌های بازدارنده‌ای از جمله توسعه اعتماد نسبت به یک محیط تجارت الکترونیکی، به عنوان نیروی محرکه در این زمینه مواجه می‌باشند. همچنین مکانیسم‌های کنترلی سفت و سخت، قیمت محصولات و خدمات را به دلیل ضمانت هزینه بیشتر به عنوان هزینه عملیاتی، بر اساس نوع مکانیسم‌های کنترلی، افزایش می‌دهد.

مصرف‌کنندگان از یک محیط تجارت الکترونیکی، رفتار قابل اعتماد از وب یا آن محیط الکترونیکی نیاز دارند. با این حال، بسیاری از مصرف‌کنندگان به دلیل پیچیده بودن تکنولوژی اقدامات کنترلی، در محیط‌های الکترونیکی شکایت می‌کنند. چراکه معتقدند عملکرد عملیاتی آن‌ها را تحت تاثیر قرار می‌دهد. به عنوان مثال مشتریان زیادی به دلیل پیچیدگی با چالش زمان پاسخگویی بیشتر در پردازش سفارش‌های خود مواجه هستند، اگرچه تاثیر آن هنوز نامشخص است.

مدیران محیط‌های تجارت الکترونیکی از اقدامات امنیتی رضایت کافی را ندارند. معتقدند امروزه، گاهی اوقات مصرف‌کنندگان دوست ندارند کالای خود را به صورت آنلاین بخرند، زیرا آن‌ها احساس می‌کنند که سیستم بیش از حد وقت گیر است؛ بنابراین لازم است تعادل بین اقدامات کنترلی و عملکرد عملیاتی به عنوان یک راهبرد سیاستی مورد توجه قرار گیرد. در مقابل نظر دیگر این است که پس از تشدید و به کارگیری اقدامات امنیتی و کنترلی در فضای آنلاین، نه تنها مشکلی به وجود نمی‌آید بلکه منجر به افزایش اعتماد مشتریان احتمالی می‌شود؛ بنابراین از آنجایی که پیاده‌سازی ابزارهای کنترلی مختلف فرآیندی تدریجی است، تاثیر جامع این سه پدیده بر قصد خرید کلی مصرف‌کنندگان از یک محیط تجارت الکترونیکی هنوز به خوبی تثبیت و شناسایی نشده است. در این راستا تحقیقات سیستماتیک و کاملاً تجربی باید برای برآورد هدف نهایی، یعنی قصد خرید مصرف‌کنندگان در یک محیط تجارت الکترونیکی انجام شود.

بر اساس بحث فوق، این مطالعه زیربنای دستاورد خود را معطوف به این سوال می‌کند که پس از به کارگیری اقدامات مختلف مدیریتی و فناوری برای کنترل سرقت هویت و خطرات مرتبط با آن، تاثیر عملکرد عملیاتی، اعتماد و قیمت محصولات/خدمات بر قصد خرید مصرف‌کنندگان در یک محیط تجارت الکترونیکی یا آنلاین چیست؟ با این اوصاف ابتدا به تبیین فرضیه‌های تحقیق پرداخته و سپس یک نمای کلی از مدل پیشنهادی در راستای هدایت جنبه‌های تجربی تحقیق، ارایه و مورد بحث و تبیین قرار می‌گیرد. دلایل تبیین و توسعه فرضیه‌های مرتبط با تعامل و روابط قصد خرید با اعتماد درک شده، ارزش قیمت درک شده و عملکرد عملیاتی به شرح زیر ارایه می‌گردد.

البته اعتماد درک شده توسط سه مولفه شامل امنیت درک شده، حریم خصوصی درک شده و اضطراب درک شده و عملکرد عملیاتی تحت تاثیر ارزش زمانی درک شده و ارزش تلاش درک شده قرار می‌گیرد [7]، [8]، [20]، [21].

۱-۲- اعتماد درک شده (از سرقت هویت)

اعتماد عبارت است از اطمینان کلی مصرف‌کنندگان در مورد اعتبار و قابلیت اعتماد فروشندگان که طی آن ارزش‌های مورد انتظار مصرف‌کنندگان هنگام تبادل مالی، فیزیکی و روانی برآورده می‌شود [22]، [23]. سازگاری و به روز شدن با ویژگی‌های پویای یک کانال خرید آنلاین، باعث علاقه زیاد مصرف‌کنندگان به خرید در چنین فضایی می‌شود [9]، [11] اما، مصرف‌کنندگان زیادی وجود دارند که تنها به دلیل عدم اعتماد به چنین فضایی از خرید آنلاینی خودداری می‌کنند [10]، [24]، [25]. مطالعه حاضر همسو با بسیاری از مطالعات علمی [11]، [16]، [21] استدلال می‌کند که استفاده از ابزارهای کنترلی سرقت هویت بر ادراک فزاینده اعتماد که قصد خرید مشتریان را از یک محیط تجارت الکترونیکی دنبال می‌کند، تشدید کرده است. از این رو، امنیت سایت، امنیت عملیاتی، نگرش شخصی و امنیت محیطی محلی از عوامل اصلی شکل‌گیری اعتماد درک شده در بین مصرف‌کنندگان است. مطالعات در مورد فعالیت در یک محیط تجارت الکترونیکی و نگرش مصرف‌کنندگان [7]، [9]، [13]، [14] نشان می‌دهد که اعتماد درک شده به شدت با درک مصرف‌کنندگان از قابلیت اطمینان و اصالت و اعتبار سایت ارتباط دارد. برای تحقق هدف پژوهش، بر اساس مرور ادبیات مفهومی تعریف اعتماد [7]، [11]، [13] اعتماد درک شده را می‌توان به میزان درجه اعتماد شناختی، عاطفی و رفتاری مصرف‌کنندگان به فروشندگان الکترونیکی به دلیل استفاده از اعمال مکانیسم‌های سرقت هویت که تعاملات و تراکنش‌های آن‌ها در یک محیط تجارت الکترونیکی را از هرگونه خطری که ممکن است از حملات هکرها ناشی شود محافظت کند، تعریف کرد؛ بنابراین با توجه به مباحث فوق، فرضیه زیر پیشنهاد می‌شود.

H_1 : اعتماد درک شده تاثیر مثبت معناداری بر قصد خرید مصرف‌کنندگان از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

۱-۱-۲- اضطراب درک شده (از سرقت هویت)

رویکرد هزینه مبادله نشان داد که نا اطمینانی در هر معامله‌ای آثار سوزیادی بر وضعیت روحی روانی مصرف‌کنندگان دارد. محققان [13]، [14]، [17] نشان دادند که فعالیت در محیط تجارت الکترونیکی که در آن هر تراکنش با درجه خاصی از نا اطمینانی همراه است، همیشه نوعی اضطراب را در ذهن مصرف‌کنندگان ایجاد می‌کند و به‌نوعی از نظر روانی، عصبانیت و بی‌ثباتی به دنبال خواهد داشت [24]، [25]. با این حال، اعمال اقدامات کنترلی سرقت هویت به‌طور بالقوه می‌تواند بی‌ثباتی روانی را کاهش داده و اضطراب ذهنی را از بین ببرد [21]. با بررسی مطالعات مرتبط با نگرش اعتماد [11]، [16] می‌توان استدلال کرد که اعتماد مرتبط با سرقت هویت به‌طور قابل ملاحظه و معناداری با اضطراب درک شده مرتبط است [3]، [9]، [16].

این اضطراب درک شده می‌تواند تحت تاثیر درک امنیت و حریم خصوصی قرار گیرد؛ بنابراین، این مطالعه، مرور ادبیات را ساده می‌کند [5]، [14]، [16]، [17]، [26] و اضطراب درک شده را به‌عنوان موضوعی در نظر می‌گیرد که مصرف‌کنندگان می‌توانند از نظر روانی، با کاهش عذاب روحی و استرس در تعاملات و معاملات در یک محیط تجارت الکترونیکی، متاثر از خطرات ناشی از حمله هکرها به دلیل اعمال مکانیسم‌های کنترل سرقت هویت مفهوم‌سازی کند. در این ارتباط فرضیه زیر پیشنهاد می‌گردد:

H_2 : اضطراب درک شده تاثیر معناداری بر اعتماد درک شده هنگام خرید از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل‌کننده سرقت هویت دارد.

۲-۱-۲- امنیت درک شده (از سرقت هویت)

محافظت در برابر خطرات مالی (کلاهبرداری پولی) و اجتماعی (ترس از دست دادن موقعیت اجتماعی به دلیل ناتوانی در حفظ ارتباط با بسیاری از آژانس‌های اجتماعی پس از دست دادن اطلاعات هویتی خود توسط هکرها هنگام خرید، به‌عنوان درک کلی از امنیت طبقه‌بندی می‌شود [7]، [8]. از سوی دیگر، ادراک خطرات روانی و اضطراب ناشی از سرخوردگی شدید ذهنی به دلیل از دست دادن اطلاعات هویتی و رنج‌های مرتبط با آن می‌تواند در هنگام خرید از یک محیط نامطمئن، اضطراب را در بین مصرف‌کنندگان ایجاد کند [9]، [13]، [14]؛ بنابراین، رفع گسترده زمینه‌های خطراتی مرتبط با اجرای اقدامات کنترل سرقت هویت، می‌تواند به مشارکت و افزایش اعتماد مشتریان در قصد خرید منجر شود و به‌عنوان امنیت درک شده طبقه‌بندی شود. وقتی که مشتریان تشخیص می‌دهند که ابزارهای مختلف کنترلی مدیریتی و فناوری به‌منظور محافظت از آن‌ها در برابر خطرات مالی، روانی و اجتماعی اجرا می‌شود، درک امنیت از محیط تجارت الکترونیکی برایشان ایجاد می‌شود که در نهایت به اعتماد آن‌ها کمک می‌کند. ویژگی‌های امنیتی و کنترلی وب‌سایت‌ها و شهرت فروشندگان می‌تواند باعث افزایش اعتماد درک شده مصرف‌کنندگان شود که قصد رفتاری آن‌ها را به نفع خرید آنلاین ساده می‌کند. لذا با توجه به مباحث ارایه‌شده، فرضیه زیر پیشنهاد می‌شود.

H_3 : امنیت درک شده تاثیر مثبت معناداری بر اعتماد درک شده توسط مصرف‌کنندگان هنگام خرید از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت است.

۳-۱-۲- حریم خصوصی درک شده (از سرقت هویت)

ریسک‌های درک شده می‌تواند از جنبه‌های مختلفی مانند عملکرد، مالی، زمانی، روان‌شناختی، اجتماعی و حریم خصوصی ناشی شود [3]. با این حال، از آنجایی که مطالعه حاضر تنها بخشی از اعتماد را بررسی می‌کند که به دلیل اعمال اقدامات کنترلی سرقت هویت ایجاد شده است، تنها خطرات مرتبط با جنبه‌های مالی، اجتماعی، روانی و حریم خصوصی در نظر گرفته می‌شود. پس از اعمال بسیاری از مکانیسم‌های کنترلی سرقت هویت، مشتریان ممکن است احساس کنند که هکرها نمی‌توانند اطلاعات شخصی را که در حین خرید از وب‌سایت‌ها افشا و به اشتراک گذاشته

می‌شود، استخراج کنند و این انگیزه می‌تواند درک آن‌ها از حریم خصوصی را افزایش دهد که منجر به تغییر نگرش مشتریان نسبت به اعتماد به خرید در یک محیط تجارت الکترونیکی می‌شود و درک آن‌ها از اضطراب را کاهش می‌دهد؛ لذا فرضیه پیشنهادی در این زمینه عبارت‌اند از:

H_4 : حریم خصوصی درک شده تاثیر مثبت معناداری بر اعتماد درک شده مصرف‌کنندگان هنگام خرید از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

۲-۲- ارزش قیمت درک شده (از سرقت هویت)

هنگام تعامل و ارایه اطلاعات شخصی به وبسایت‌ها، خطرات مالی قابل توجه و بالقوه‌ای وجود دارد [7]، [8]. مطالعات [13]، [14]، [17] نشان داده‌اند که به‌طور بالقوه در بلندمدت در یک محیط تجارت الکترونیکی، کلاهبرداری‌های مالی یا هویتی را به دلیل حملات تهاجمی هکرها تجربه می‌کنند. همچنین پیشنهاد کرده‌اند که خطرات مالی، روانی و اجتماعی ناشی از سرقت هویت می‌تواند به‌شدت مصرف‌کنندگان را از دنبال کردن قصد مثبت خرید، منصرف کند. از سوی دیگر، اعمال اقدامات کنترلی مختلف سرقت هویت به‌طور بالقوه می‌تواند خطر از دست دادن اطلاعات شخصی خصوصی از جمله شماره کارت اعتباری و ضرر مالی ناشی از کلاهبرداری را کاهش دهد، در نتیجه می‌تواند موجب صرفه‌جویی و پس‌انداز پول شود آلفورد [27] در مطالعه خود نشان داد که معمولاً، مصرف‌کنندگان هنگام ابراز تمایل به خرید، مبادله قیمت-ارزش می‌کنند. بر اساس نظریه یکپارچه پذیرش و استفاده از فناوری، دودز و همکاران [28] تایید کردند که تمایل مصرف‌کنندگان به ارزیابی ارزشی که در ازای پولی که خرج می‌کنند به‌دست می‌آورند، می‌تواند قصد خرید آن‌ها را به کانال‌های مبتنی بر فناوری اطلاعات و ارتباطات هدایت کند. از این رو، فرضیه‌ای به شرح زیر تبیین می‌شود.

H_5 : ارزش قیمت درک شده تاثیر مثبت معناداری بر قصد خرید مصرف‌کنندگان از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

۲-۳- عملکرد عملیاتی

با توجه به مدل پیشگیری-منبع در یک محیط تجارت الکترونیکی [21]، اقدامات اداری مانند کنترل کارکنان، اعمال قوانین و مقررات تشدیدکننده و سیاست‌های مدیریتی می‌تواند منجر به کاهش و به حداقل رساندن احتمال تهدید سرقت هویت شود. هرچند انعطاف‌پذیری مرتبط با تعامل بین کامپیوتر و کاربر در محدوده سیستم‌ها، سیاست‌ها و مقررات تحت تاثیر قرار گیرند. تاثیرات اصول اداری می‌تواند موانع زیادی بین روابط محیط مجازی/آنلاین و مشتریان راه دور، ایجاد کند [21]. نظریه یکپارچه پذیرش و استفاده از فناوری (UTAUT) [29]، عملکرد عملیاتی را از طریق اثر ترکیبی انتظار عملکرد و انتظار تلاش، اندازه‌گیری کرده است [30]؛ بنابراین می‌توان ادعا کرد که تغییر بالقوه در سطح عملکرد عملیاتی، ممکن است تاثیر ترکیبی شدیدی بر پذیرش مصرف‌کنندگان نسبت به فعالیت در محیط تجارت الکترونیکی داشته باشد [31]. با وام گرفتن از ماهیت ساختار عملکرد عملیاتی درک شده از مطالعه [21]، دو بعد آن یعنی ارزش زمانی و ارزش تلاش را به‌عنوان میزان زمان و تلاش درک شده موردنیاز برای به سرانجام رسیدن هدف نشانه‌گذاری شده از سوی مصرف‌کننده، مفهوم‌سازی کرد. از این رو، فرضیه پیشنهادشده عبارت است از:

H_6 : عملکرد عملیاتی تاثیر مثبت معناداری بر قصد خرید مصرف‌کنندگان از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

۲-۳-۱- ارزش زمانی درک شده (از سرقت هویت)

از ساختار یا سازه کارایی زمانی، که در رویکرد هزینه معامله، مفهوم‌سازی شده است، می‌توان برای درک مصرف‌کنندگان از ارزش به‌دست آمده در ازای زمان سرمایه‌گذاری شده برای دستیابی به هدف موردنظر، درک روشن و عمیقی دریافت نمود [26]، [32]. البته این نگرانی جدی است که کنترل تهدیدات امنیتی با به‌کارگیری اقدامات مدیریتی و فناوری می‌تواند منجر به مصرف زمان بیشتر برای تحقق اهداف موردنظر از طریق تعامل با وبسایت یک محیط تجارت الکترونیکی شود [2]، [11]، [32]. در مدل پذیرش سلامت تلفن همراه [2]، نشان داده است که زمان انتظار، به‌عنوان مثال، بازگشت ارزش زمان، یکی از نگرانی‌های غالب برای مصرف‌کنندگان برای پذیرش یا عدم پذیرش هرگونه رسانه مجازی تحت کنترل

ICT است. در تجزیه و تحلیل هزینه تراکنش، نیز قصد رفتاری مصرف کنندگان برای یافتن مقایسه ارزشی برحسب تلاش سرمایه گذاری شده و بازده به دست آمده منعکس شده است. در نتیجه مصرف زمان اضافی می تواند باعث درک عملکرد کمتر وبسایت شود؛ بنابراین ارزش زمانی درک شده به عنوان درجه ای از ارزش شناختی و عاطفی مطلوب که از طریق تعامل در یک محیط تجارت الکترونیکی در ازای صرف زمان انجام تبادل مصرف کنندگان، در نظر گرفته می شود. در این راستا، این می توان فرضیه زیر را در نظر گرفت:

H₇: ارزش زمانی درک شده تاثیر مثبت معناداری بر ادراک مصرف کنندگان از عملکرد عملیاتی در خرید از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

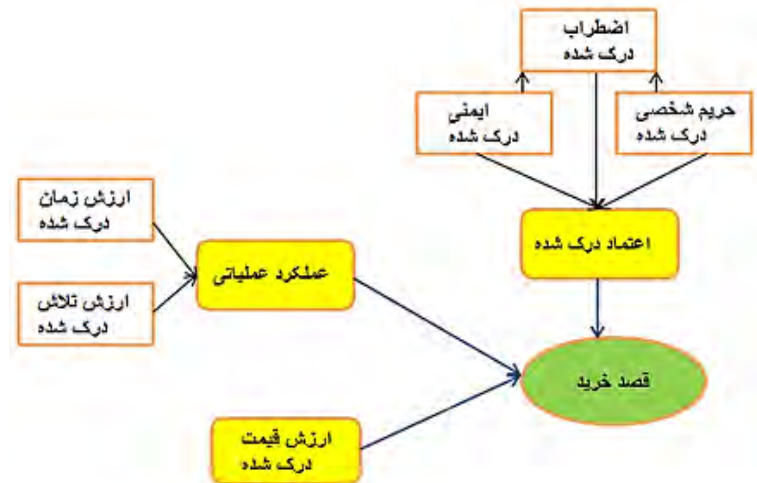
۲-۳-۲- ارزش تلاش درک شده (از سرقت هویت)

بر اساس نظریه اشاعه نوآوری [4]، [33] و مدل پذیرش فناوری [34] و بسیاری از کارهای اساسی در مورد پذیرش مصرف کننده [2]، پذیرش هرگونه فناوری مبتنی بر محیط مجازی به طور قابل ملاحظه و معناداری با درک مصرف کنندگان از درک آسان و تعامل با آن سیستم، ارتباط دارد. پذیرش یک رسانه مجازی توسط مصرف کنندگان ریشه در چهار جنبه رفتاری دارد که عبارت اند از تمایل به استفاده (یعنی، نگرش و انگیزه)، توانایی استفاده، استدلال برای استفاده و رضایت از استفاده، که به اتفاق، ارزیابی پیچیدگی سیستم را نشان می دهد.

با توجه به نظریه اشاعه نوآوری [33] و سهولت استفاده درک شده از مدل پذیرش فناوری [34]، پیچیدگی، می تواند معنی مفهومی تلاش مورد نیاز مصرف کنندگان برای انجام وظیفه مورد نظر خود را تعریف کند و می توان آن را به عنوان درجه ای که مصرف کنندگان، ارزش شناختی و عاطفی مورد نظر را از طریق تعامل در یک محیط تجارت الکترونیکی به دست می آورند که منعکس کننده مشکلات در درک و استفاده در انجام وظیفه مورد نظر است، تعریف کرد. از این رو، فرضیه پیشنهادی عبارت است از:

H₈: ارزش تلاش درک شده تاثیر مثبت معناداری بر ادراک مصرف کنندگان از عملکرد عملیاتی در خرید از یک محیط تجارت الکترونیکی با توجه به اعمال اقدامات کنترل سرقت هویت دارد.

نهایتاً بر اساس فرضیه های ذکر شده، مدل تحقیق پیشنهادی در شکل زیر نشان داده شده است. مدل فرض می کند که عملکرد عملیاتی، ارزش قیمت درک شده و اعتماد درک شده مستقیماً بر قصد خرید، تاثیر دارد اما خود میانجی مولفه های دیگرند به این قرار که اعتماد درک شده، میانجی اضطراب، امنیت و حریم شخصی درک شده بوده و عملکرد عملیاتی، میانجی ارزش زمان و ارزش تلاش درک شده بر قصد خرید آنلاینی در نظر گرفته شده است؛ بنابراین، مدل نشان می دهد که چگونه، مکانیسم های کنترل سرقت هویت، می تواند قصد خرید در یک محیط تجارت الکترونیکی یا آنلاینی را تحت تاثیر قرار دهد.



شکل ۱- تاثیر مکانیسم‌های کنترلی سرقت هویت بر قصد خرید آنلاین، یک محیط تجارت الکترونیکی در مدل IT-OPI [1].

Figure 1- The effect of identity theft control mechanisms on the intention to buy online, an e-commerce environment in IT-OPI model [1].

۳- روش‌شناسی

پژوهش حاضر در دو بخش نظری و میدانی صورت گرفته است. بخش نظری آن مبتنی بر مطالعات کتابخانه‌ای بوده که ضمن گردآوری و فیش‌برداری مقالات و متون مربوطه، به جمع‌بندی و دسته‌بندی نظریات مختلف پرداخته شده است. برای جمع‌آوری داده‌های مربوط به مبانی نظری و استخراج عوامل و شاخص‌های اولیه از منابع کتابخانه‌ای و اینترنتی شامل کتب، مقالات و مطالعات موردی استفاده شده است. جهت گردآوری اطلاعات و داده‌های موردنیاز به منظور بررسی فرضیه‌های تحقیق از پرسشنامه استاندارد بهره‌گیری شد. در این ارتباط یک رویکرد تجربی برای بررسی تاثیر سه سازه یا مولفه مشارکت‌کننده در مورد قصد خرید یک محیط تجارت الکترونیکی به کار گرفته شده است.

ابزار مورد استفاده روش میدانی در این پژوهش، پرسشنامه استاندارد با مقیاس لیکرت ۵ درجه‌ای از ۱ (کاملاً مخالفم/هرگز) تا ۵ (کاملاً موافق/همیشه) و شامل دو بخش می‌باشد. آیتم‌های اندازه‌گیری برای هر دو متغیر مستقل و وابسته از ادبیات موجود اقتباس شدند. برای اندازه‌گیری متغیرهای مستقل و ابعاد آن از ۳۷ گویه و برای اندازه‌گیری متغیر وابسته ۴ مورد از آیتم‌ها استفاده می‌شود. یک گروه متمرکز متشکل از اساتید دانشگاه با تخصص مرتبط با بازاریابی و دو متخصص (مدیران سطح بالا) که تجربه وسیعی در عملیات یک محیط تجارت الکترونیکی داشتند، پرسشنامه را برای اعتبار روایی بررسی خواهند کرد.

سپس پرسشنامه توسط ۲۰ نفر از اساتید یک محیط تجارت الکترونیکی مورد بررسی و آزمون قرار می‌گیرد. از طریق یک مصاحبه کوتاه با ۶۵۰ دانشجوی رشته مدیریت بازرگانی دانشگاه آزاد اسلامی واحد علوم تحقیقات تهران، ۲۴۲ دانشجو که تقریباً ماهی یک‌بار به صورت آنلاین خرید دارند، انتخاب شدند. از بین ۲۴۲ دانشجو، ۲۰۰ نفر را با تقسیم‌بندی مساوی جنسیتی با توجه به تجربه قبلی آن‌ها در خرید از یک محیط تجارت الکترونیکی و تناوب تعامل با وبسایت‌های مختلف یک محیط تجارت الکترونیکی به صورت تصادفی انتخاب شدند. پس از جمع‌آوری ۳۰ پرسشنامه آزمایشی، پایایی و نرمالیتی داده‌های مولفه‌های پرسشنامه با استفاده از معیار آلفای کرونباخ و آماره K-S در نرم‌افزار SPSS مورد بررسی قرار گرفت. همچنین جهت تجزیه و تحلیل داده‌ها و تعیین مسیر و ضرایب آن از نرم‌افزار PLS استفاده شده است.

جدول ۱- آزمون‌های مرتبط با پرسشنامه.

Table 1- Tests related to the questionnaire.

ابعد	تعداد گویه (حذف شده)	آلفای کرونباخ	K-S
عملکرد عملیاتی OP	(2) 4	0.78	0.872
ارزش تلاش درک شده PEV	(2) 3	0.76	0.657
ارزش زمان درک شده PTV	(2) 3	0.87	0.834
اعتماد درک شده PT	(2) 3	0.89	0.932
امنیت درک شده PS	(0) 4	0.75	0.568
اضطراب درک شده PA	(2) 3	0.79	0.468
حریم خصوصی درک شده PP	(1) 3	0.85	0.765
ارزش قیمت درک شده PPV	(2) 3	0.88	0.693
قصد خرید PI	(0) 4	0.76	0.739

جدول ۲- آمار توصیفی متغیرهای پژوهش.

Table 2- Descriptive statistics of research variables

مؤلفه‌ها	نماد	میانگین	انحراف معیار
عملکرد عملیاتی	OP	4.206	0.671
ارزش تلاش درک شده	PEV	4.556	0.917
ارزش زمان درک شده	PTV	4.044	0.907
اعتماد درک شده	PT	3.556	0.212
امنیت درک شده	PS	4.115	0.234
اضطراب درک شده	PA	3.987	0.918
حریم خصوصی درک شده	PP	4.654	0.976
ارزش قیمت درک شده	PPV	4.968	0.980
قصد خرید	PI	4.012	0.895

در این مطالعه از طریق معادلات ساختاری ضرایب مسیر برآورد شدند و جهت تجزیه و تحلیل دقیق‌تر متغیر میانجی با روش سوبل برای هر مسیر محاسبه گردید (در اکثر قریب به اتفاق تحقیقات برای تحلیل میانجی از آماره Z -value که یک فرمول منسوخ شده و ضعیفی می‌باشد، استفاده شده و یا متأسفانه هنوز مورد استفاده قرار می‌گیرد). مطابق با تعریف بارون و کنی، متغیر میانجی متغیری است که تمام یا بخشی از اثر متغیر مستقل بر وابسته را منوط به خود می‌کند. اشتباه دقیقا از عدم توجه به همین نکته شروع می‌شود؛ یعنی (تمام یا بخشی از اثر متغیر مستقل بر وابسته)، یعنی باید اثری بین این دو متغیر باشد که متغیر واسطه یا میانجی بتواند بخشی یا تمام آن را از خود عبور دهد. تاکید می‌گردد که نباید تاثیر غیرمستقیم را با اثر میانجی اشتباه گرفت. دو روش اصلی بارون و کنی و بوت استرپینگ سوبل به عنوان دو روشی است که بیش از ۹۸٪ پژوهش‌های جهان با این دو روش خلاقانه تحلیل می‌شود.

علیرغم اینکه سوبل روش خود را بعدا با روش بوت استرپینگ کاملا بروز کرد و ایرادات روش اولیه را برطرف نمود، اما هنوز در مطالعات از آماره Z -value با فرمولی ضعیف برای تحلیل میانجی هستند؛ بنابراین علاوه بر نبود مطالعات مرتبط با سرقت هویت، تحلیل میانجی سوبل نوآوری دیگر مطالعه می‌باشد. مدل ساختاری روابط علی متغیرهای پنهان مستقل با متغیر وابسته را از همان روشی که در فرضیه‌ها بیان می‌شود، تایید می‌کند. با این حال، قبل از اقدام به آزمون فرضیه، بحث در مورد درون‌زایی بسیار مهم است. چراکه ممکن است بر نتیجه پیش‌بینی متغیر وابسته با اثر متقابل سازه‌های مستقل تاثیر مرکب بگذارد [35]. از آنجایی که برای جمع‌آوری داده‌ها از طریق آزمایش تصادفی، احتمال درون‌زایی کاهش می‌یابد [36]، علت اثر متغیرهای برون‌زا بر متغیر درون‌زا پیش‌بینی و درنهایت از طریق حمایت از بررسی ادبیات و نظریه‌ها استخراج می‌شود؛ بنابراین می‌توان ادعا کرد که درون‌زایی یک موضوع بالقوه برای این مطالعه نیست [37]. تحلیل رابطه علت و معلولی نشان داد که مدل به اندازه کافی برازش دارد.

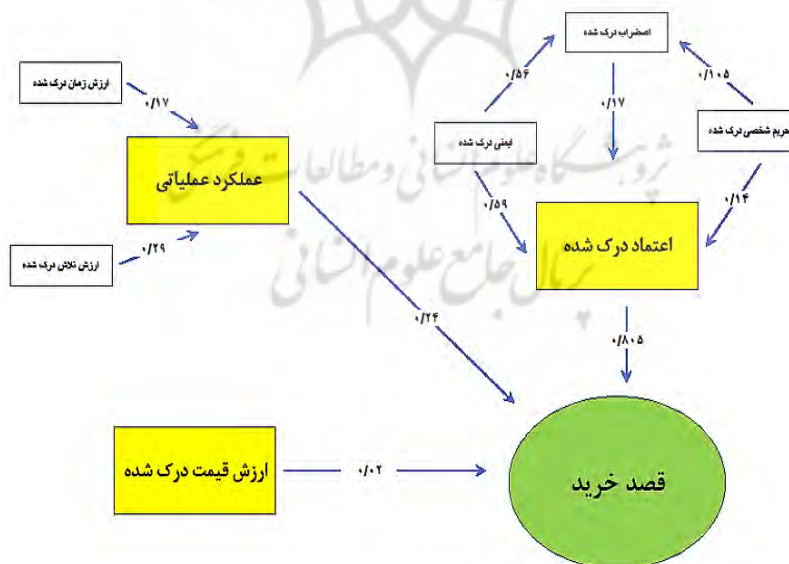
شاخص‌های (CFI)، شاخص خوبی برازش^۱، ریشه میانگین مربعات خطای تقریب^۲، شاخص برازش تنظیم‌شده^۳، شاخص برازش نرمال^۴، شاخص برازش افزایشی^۵ و شاخص تناسب نسبی^۶ [38]، [39].

مدل برازش شده با داده‌های منطبق با ادبیات و مبانی نظری نشان داد که تمامی روابط فرضی غیر از دو رابطه معنادار هستند. یکی ارزش قیمت درک شده^۷ رابطه معنی‌داری با قصد خرید ندارد و دیگری حریم خصوصی درک شده^۸ تاثیر معنی‌داری بر درک از اضطراب^۹ ندارد. به نظر نمی‌رسد که این دو مسیر ارتباط قابل توجهی در قصد خرید داشته باشند قصد و اضطراب به ترتیب در سطوح ۰/۰۵ و حتی در سطوح ۰/۱۰، غیرمعنادار است. جدول ۳ شاخص‌های تناسب مدل را نشان می‌دهد. همچنین نتایج آزمون فرضیه‌ها در جدول ۴ تا جدول ۶ بیان شده است. شکل‌های ۳ لغایت ۵ نیز نشان دهنده نتایج آزمون سوبل می‌باشد.

جدول ۳- شاخص‌های تناسب مدل.

Table 3- Model fit indices.

اندازه‌گیری مناسب	توصیه شده	معتبر
کای دو χ^2	$0.05 \leq P$	0.297 (15.6)
درجات آزادی df		16
کای دو بخش بر درجات آزادی χ^2/df	≤ 3.00	1.18
شاخص برازش تطبیقی CFI	≥ 0.90	0.987
شاخص نیکویی برازش CFG	≥ 0.90	0.984
ریشه میانگین مربعات خطای برآورد RMSEA	≥ 0.061	0.031
شاخص نیکویی برازش تعدیل شده	≥ 0.80	0.932
شاخص برازش نرمال شده NFI	≥ 0.91	0.987
شاخص برازش افزایشی IFI	≥ 0.91	0.992
شاخص برازش نسبی RFI	≥ 0.80	0.941



شکل ۲- مدل استخراج شده از نرم افزار PLS.

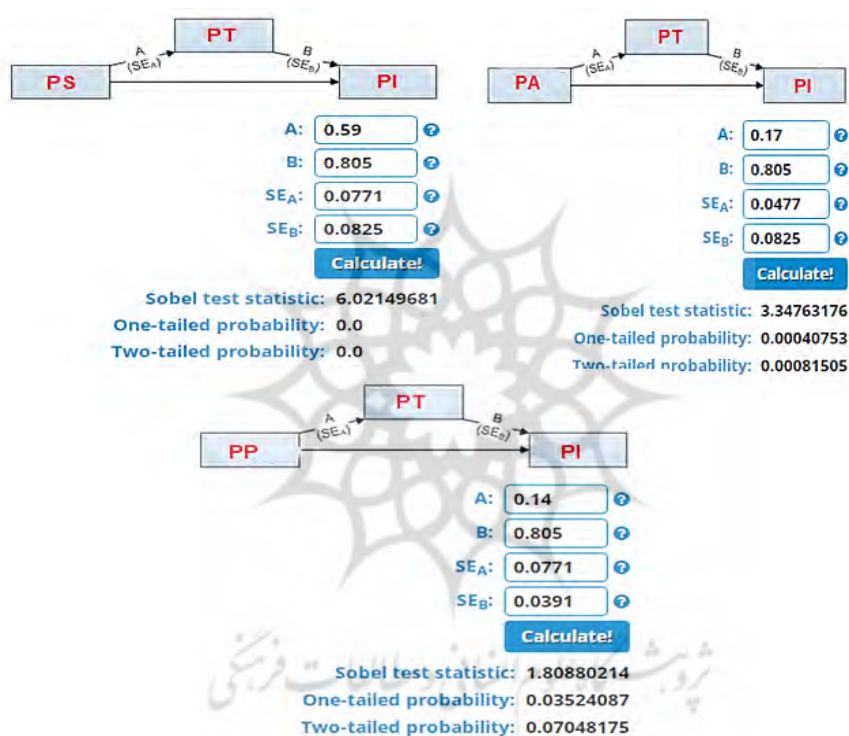
Figure 2- Model extracted from PLS software.

¹ Goodness of Fit Index (GFI)² Root Mean Square of the Approximation Error (RMSAE)³ Adjusted Fit Index (AFI)⁴ Normal Fit Index (NFI)⁵ Incremental Fitness Index (IFI)⁶ Relative Fit Index (RFI)⁷ Perceived Price Value (PPV)⁸ Perceived privacy (PP)⁹ Perception Anxiety (PA)

جدول ۴- نتایج آزمون فرضیه‌های پژوهش (فرضیه اول).

Table 4- The results of the test of the research hypotheses (H1).

فرضیه	تایید/رد	ضریب	Z	Sobel
H ₁ با توجه به به‌کارگیری اقدامات کنترل سرقت هویت، اعتماد درک شده تاثیر مثبت معناداری بر قصد خرید مصرف‌کنندگان در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده	0.805	9.756	----
H ₁₁ با توجه به اعمال اقدامات کنترل سرقت هویت، اضطراب ادراک شده بر درک مصرف‌کنندگان از اعتماد هنگام خرید در یک محیط تجارت الکترونیکی تاثیر می‌گذارد.	تایید شده	0.170	3.561	3.347
H ₁₂ با توجه به استفاده از اقدامات کنترل سرقت هویت، امنیت درک شده تاثیر مثبت معناداری بر درک مصرف‌کنندگان از اعتماد هنگام خرید در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده	0.590	7.649	6.021
H ₁₃ با توجه به اعمال اقدامات کنترل سرقت هویت، حریم خصوصی درک شده تاثیر مثبت معناداری بر درک مصرف‌کنندگان از اعتماد هنگام خرید در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده با احتیاط	0.140	3.573	1.808



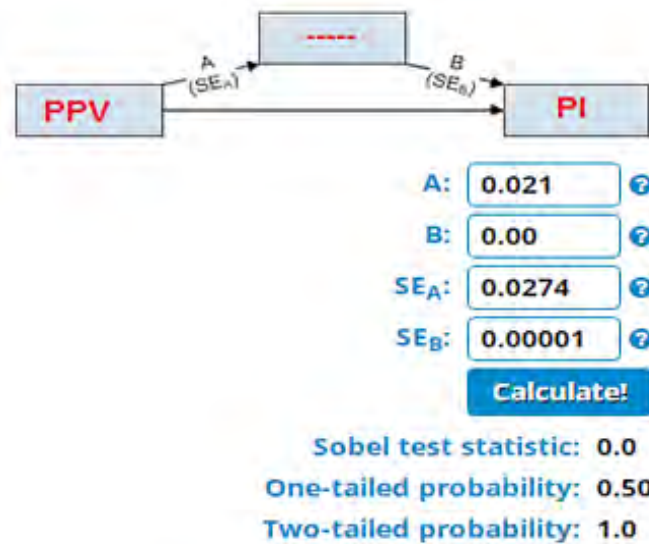
شکل ۳- نتایج آزمون آزمون سوبل (فرضیه اول).

Figure 3- The results of the test of Sobel (H1).

جدول ۵- نتایج آزمون فرضیه‌های پژوهش (فرضیه دوم).

Table 5- The results of the test of the research hypotheses (H2).

فرضیه	تایید/رد	ضریب	Z	Sobel
H ₂ با توجه به اعمال اقدامات کنترل سرقت هویت، ارزش قیمت درک شده تاثیر مثبت معناداری بر قصد خرید مصرف‌کنندگان در یک محیط تجارت الکترونیکی یا آنلاین دارد.	رد شده	0.021	0.764	

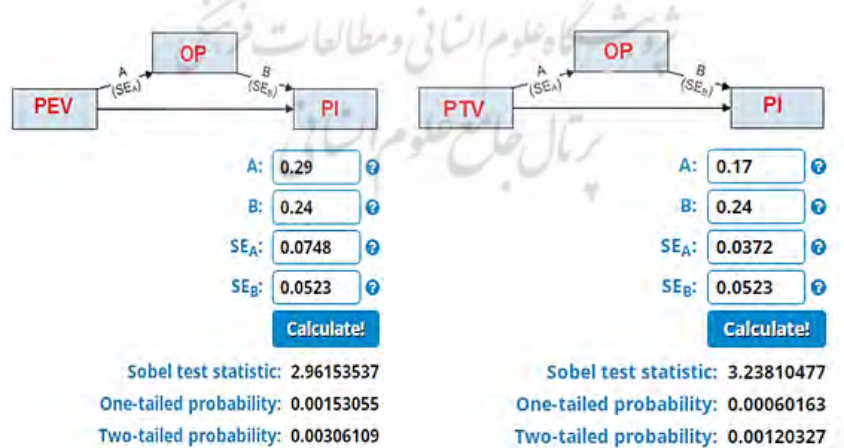


شکل ۴- نتایج آزمون آزمون سوبل (فرضیه دوم).
Figure 4- The results of the test of Sobel (H2).

جدول ۶- نتایج آزمون فرضیه‌های پژوهش (فرضیه سوم).

Table 6- The results of the test of the research hypotheses (H3).

فرضیه	تایید/رد	ضریب	Z	Sobel
H ₃ با توجه به به کارگیری اقدامات کنترل سرقت هویت، عملکرد عملیاتی تاثیر مثبت معناداری بر قصد خرید مصرف کنندگان در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده	0.240	4.581	-----
H ₃₁ با توجه به استفاده از اقدامات کنترل سرقت هویت، ارزش زمانی درک شده تاثیر مثبت معناداری بر درک مصرف کنندگان از عملکرد عملیاتی هنگام خرید در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده	0.170	4.562	3.238
H ₃₂ با توجه به استفاده از اقدامات کنترل سرقت هویت، ارزش تلاش درک شده تاثیر مثبت معناداری بر درک مصرف کنندگان از عملکرد عملیاتی هنگام خرید در یک محیط تجارت الکترونیکی یا آنلاین دارد.	تایید شده	0.290	3.876	2.961



شکل ۵- نتایج آزمون آزمون سوبل (فرضیه سوم).
Figure 5- The results of the test of Sobel (H3).

۴- یافته‌های حاصل از تخمین مدل‌ها

مجذور ضریب همبستگی چندگانه نشان می‌دهد ۸۹٪ تغییرات قصد خرید را می‌توان با عملکرد عملیات، اعتماد درک شده و ارزش قیمت درک شده توضیح داد. مقدار بالاتر این ضریب حکایت از این دارد که سازه‌ها برای سنجش و اندازه‌گیری سازه وابسته به اندازه کافی با ساختارها مطابقت دارد. برای رابطه علی، اعتماد درک شده با امنیت درک شده، اضطراب درک شده و حریم خصوصی درک شده، ۶۶/۳٪ تغییرات اعتماد درک شده در یک محیط تجارت الکترونیکی یا آنلاین را در برابر سرقت هویت یا هر جرم سایبری دیگری، با این سه سازه توضیح داده می‌شود. همچنین ۴۷/۴٪ تغییرات عملکرد عملیاتی توسط دو سازه ارزش زمان درک شده و ارزش تلاش درک شده توضیح داده می‌شود. از بین سه سازه فرضی که قصد خرید را شکل می‌دهند، اعتماد درک شده در خصوص تعامل و تراکش ایمن در خرید از یک محیط تجارت الکترونیکی بیشترین سهم را دارد (۰/۸۰۵).

به این معنا که هنگامی که اثر عملکرد عملیاتی و ارزش قیمت ثابت می‌مانند، یک واحد تغییر در اعتماد درک شده باعث تغییر ۰/۸۰۵ واحد تغییر در قصد خرید مصرف‌کننده می‌شود. از سوی دیگر، اگرچه فرض بر این است که اعتماد درک شده متشکل از درک امنیت، درک حریم خصوصی و درک اضطراب در برابر جرایم سایبری است، مشاهده می‌شود که اعتماد به تبادل در یک محیط تجارت الکترونیکی یا آنلاین در حین استفاده از هویت شخصی و اطلاعات مالی حساس به دلیل استفاده از مکانیسم‌های کنترل سرقت هویت در مقایسه با ادراک بالاتر از حریم خصوصی (۰/۱۳۷) و ادراک اضطراب کمتر (۰/۱۶۶) اساساً به ادراک امنیتی (۰/۵۹۴) وابسته است. احساس عدم اطمینان در یک محیط تجارت الکترونیکی، به‌ویژه به دلیل سرقت هویت، ممکن است اثر ترکیبی شدیدی بر ذهن مصرف‌کنندگان بگذارد و اضطراب ایجاد کند [40].

درک مصرف‌کنندگان از اضطراب یک پدیده رایج در هنگام خرید از هر محیط نامطمئن است و بنابراین، می‌تواند بر نگرش اعتماد مصرف‌کنندگان تأثیر بگذارد [13]، [14]، [17]؛ بنابراین، در مقایسه با گروه اول از فرضیه‌های $(H_1, H_{11}, H_{12}, H_{13})$ ، می‌توان نتیجه گرفت که پس از اعمال مختلف مکانیسم‌های کنترل در برابر سرقت هویت، در درجه اول مصرف‌کنندگان نگران امنیت هستند، نه حریم خصوصی و اضطراب روانی و به دلیل افزایش درک امنیت، درک مصرف‌کنندگان از قابل اعتماد بودن یک محیط تجارت الکترونیکی افزایش می‌یابد که به‌طور معناداری بر قصد خرید تأثیر می‌گذارد. با اشاره به مفهوم بنیادی اقتصادی قیمت-ارزش از رویکرد هزینه معاملاتی، استدلال می‌شود که مصرف‌کنندگان همیشه صرفه‌جویی قیمت را درحالی که تراکش‌های هر تعامل را تأیید می‌کنند، ارزیابی می‌کنند.

با این حال، محققان ادعا می‌کنند که صرفه‌جویی در قیمت دلیلی بالقوه برای درک مشتریان از یک محیط تجارت الکترونیکی به‌عنوان یک کانال بازاریابی مفید و موثر است [26]، [32]. با این وجود، از زمانی که افزایش تدریجی اقدامات امنیتی برای محافظت یا به حداقل رساندن تمام خطرات مربوط به سرقت هویت می‌تواند قیمت محصول/خدمات را افزایش دهد و مقداری که مصرف‌کنندگان هنگام خرید از این کانال آسیب‌پذیر بازاریابی خرج می‌کنند [13]، [14]، طی ارزیابی بازگشت قیمت و ارزش، مصرف‌کنندگان ممکن است تصور منفی در مورد قصد خرید خود داشته باشند [26]، [41].

با این حال، در خرید یک محیط تجارت الکترونیکی، هرگونه تغییر در قیمت به دلیل اعمال بسیاری از اقدامات اداری و رمزگذاری نمی‌تواند بر قصد مصرف‌کنندگان برای خرید تأثیر بگذارد. در عوض مصرف‌کنندگان بیشتر نگران قابلیت اطمینان، اصالت و امنیت در معامله هستند. با این حال، مصرف‌کنندگان به‌طور کامل در مورد عملکرد عملیاتی نگران هستند. اگرچه مبادله قیمت و ارزش سهم قابل توجهی در بررسی مستقیم قصد خرید ندارد (برخلاف فرضیه دوم H_2)، می‌تواند بر درک مصرف‌کنندگان از عملکرد عملیاتی تأثیر بگذارد، که می‌تواند از طریق رویکرد هزینه مبادله توضیح داده شود. زمانی که مصرف‌کنندگان قیمتی را که در ازای ارزشی که به‌دست آورده‌اند، می‌پردازند به‌طور منطقی برایشان رضایت‌بخش خواهد بود؛ بنابراین آن‌ها آماده سازش با عملکرد پایین‌تر در عملیات هستند.

به دلیل انجام بسیاری از اقدامات تکنولوژیکی مانند رمزگذاری، فایروال و جاسوس یاب یا ضد جاسوس افزار (Antispyware) در یک محیط تجارت الکترونیکی، این عملیات به‌طور بالقوه می‌تواند منجر به ایجاد پیچیدگی‌های زیاد در تعامل با محیط تجارت الکترونیکی شود. از این رو با به‌کارگیری ابزارهای مختلف تکنولوژیکی و مدیریتی موثر در مدل منبع-پیشگیری، عملکرد عملیاتی می‌تواند انعطاف‌پذیری و راحتی خود را تا حد قابل توجهی از دست بدهد. مصرف‌کنندگان ممکن است با پیچیدگی‌های تکنولوژیکی و همچنین تأخیر زمانی در انجام معاملات موردنظر خود مواجه شوند چراکه به‌کارگیری ابزارهای کنترلی تا حدی تعامل آسان را از بین می‌برد. مصرف‌کنندگان همچنین ممکن است بازدهی غیر رضایت بخشی از منافع

حاصل از تعامل یک محیط تجارت الکترونیکی را از نظر ارزش زمانی درک کنند. حال باید برای تفسیر عملکرد گروه سوم فرضیه‌ها به ترکیب و سناریوی واقعی عملکرد عملیاتی توجه شود (H_{31} ، H_3 و H_{32}).

در نهایت مطالعه حاضر نگرش ادراکی مصرف‌کنندگان را به سمت خرید از یک محیط تجارت الکترونیکی موردبررسی قرار داد؛ بنابراین اقدامات کنترلی سنتی مانند کنترل‌های اداری (قرار دادن آلارم‌های قرمز در صورت وجود هرگونه سیگنال عدم تطابق رمز عبور، الگو خرید غیرمعمول، چندین خرید در مدت زمان بسیار کوتاه، مدیریت داده و ...) و اقدامات فنی مانند رمزگذاری و رمز عبور (ارتباط با بانک از طریق ارسال کد تایید در تلفن همراه ثبت شده و ...) می‌تواند در جلب اعتماد مصرف‌کنندگان و ایجاد امنیت محیط‌های الکترونیکی/آنلاینی تاثیرگذار باشد. هر چند این اقدامات پیچیدگی‌ها و سختی‌های کاربران را به‌طور قابل‌توجهی افزایش می‌دهند. عملکرد عملیاتی نیز با صرف زمان و تلاش بیشتر و همچنین قیمت بیشتر، افزایش می‌یابد. این نتایج را می‌توان از آمار توصیفی مشاهده کرد که در ادراک عملکرد عملیاتی منعکس شده است (متوسط OP برابر ۱/۷۹، میانگین PEV برابر ۲/۲۵ و PTV برابر ۲/۴۰ است). از این رو، پس از استفاده از ابزارهای کنترلی، مصرف‌کنندگان عملکرد عملیاتی بسیار پایینی را از این وبسایت‌ها، که تاثیر نامطلوبی بر قصد خرید دارد، درک می‌کنند (متوسط قصد خرید ۳/۲۹ است). با این حال، اعتماد مصرف‌کنندگان به وبسایت‌های یک محیط تجارت الکترونیکی، تضمین می‌شود (میانگین ۳/۷۱ است)، که دوباره از امنیت درک شده تشکیل شده است (میانگین ۳/۶۸) حریم خصوصی (۳/۸) و اضطراب (۳/۷۲) است. همچنین مصرف‌کنندگان این تصور را دارند که ارزش قیمت کاملاً رضایت‌بخش است (۳/۵۹)، اگرچه قیمت افزایش یافته است. با این حال، در آخر میانگین قصد خرید افزایش یافته است (بسیار بالاتر از ۳ است، یعنی آن‌ها به خرید ادامه خواهند داد) و کاملاً راضی‌کننده است؛ بنابراین استفاده از مکانیسم‌های کنترل جرایم سایبری مانند ابزارهای اداری و فناوری برای به حداقل رساندن انواع مختلف سرقت هویت، می‌تواند به‌طور بالقوه برخی از عوامل مثبت و منفی را بر ادراک مصرف‌کنندگان هنگام خرید از یک محیط تجارت الکترونیکی تحریک کند.

برنامه‌های امنیت امنیتی می‌تواند به‌طور بالقوه سرقت هویت را کاهش دهد و در نتیجه می‌تواند هزینه کلاهبرداری را کاهش دهد. با این حال، مکانیسم‌های کنترلی می‌توانند به‌طور قابل‌ملاحظه‌ای قیمت محصولات/خدمات فروخته‌شده از طریق یک محیط تجارت الکترونیکی را افزایش دهند، که در نهایت می‌تواند باعث افزایش کلی قیمت شود. این افزایش قیمت دوباره تاثیر منفی بر قصد خرید مصرف‌کنندگان از یک محیط تجارت الکترونیکی دارد. با این حال، از سوی دیگر، مصرف‌کنندگان ممکن است به دلایل زیادی از خرید آنلاین منصرف شوند، اما دلیل اصلی بازدارنده از دست دادن اعتماد به خرید آنلاین به دلیل خطرات بسیار ناشی از تهدیدات امنیتی، از دست دادن حریم خصوصی و اضطراب روانی در یک محیط مجازی است. از این رو انتظار می‌رود، استفاده از اقدامات سرقت هویت که به‌طور بالقوه خطرات مربوط به امنیت، حریم خصوصی و اضطراب را کنترل می‌کند، می‌تواند به‌طور معناداری باعث کاهش جلب اعتماد مصرف‌کنندگان به معامله یک محیط تجارت الکترونیکی شود، که در نهایت ممکن است به افزایش قصد خرید مصرف‌کنندگان منجر شود.

۵- نتیجه‌گیری و پیشنهادها

مطالعه حاضر با توجه به مدل $IT-OPI$ به بررسی ده رابطه فرضی با قصد خرید اقدام و پرداخت نمود. نتایج نشان داد که درک ارزش قیمت، یعنی افزایش جزیی قیمت خرید از محیط تجارت الکترونیکی با اعمال محدودیت اداری و مدیریت داده‌ها و اقدامات فناوری، سهم و تاثیر قابل‌توجه و معناداری در قصد خرید ندارد. از طرفی، درک مصرف‌کنندگان از عملکرد عملیاتی از سهم و تاثیر درک ارزش زمانی و درک ارزش تلاش و همچنین درک قیمت-ارزش ناشی می‌شود. اگرچه تحت تاثیر درک اعتماد درک شده نیز می‌باشد. به عبارت دیگر، اگر مصرف‌کنندگان در عملیات یک محیط تجارت الکترونیکی، اعتماد بیشتری پیدا کنند، تراکنش آنلاینی را دارای عملکرد عملیاتی بالاتر می‌دانند، اگرچه از نظر ارزش زمانی و ارزش تلاش درک شده، نسبتاً پیچیده‌تر و سخت‌تر از قبل خواهد بود. نگرش تمایل به اعتماد می‌تواند باعث ارزیابی مثبت نسبت به تجارت در فضای مجازی و الکترونیکی شود. رابطه بین حریم خصوصی درک شده و اضطراب درک شده با اعتماد نشان داد که اضطراب عمدتاً با اعتقاد و باور به امنیت در برابر هکرها کنترل می‌شود. حریم خصوصی برای مصرف‌کننده، چندان مهم نیست که نگران این عملیات باشد.

علاوه بر آن، نگرش اعتماد مصرف‌کنندگان، اگرچه متشکل از ادراکات امنیت، حریم خصوصی و فقدان اضطراب است، اما اساساً توسط امنیت درک شده کنترل می‌شود. در مجموع می‌توان نتیجه گرفت که اقدامات اداری مانند مدیریت داده‌ها، کنترل کارکنان و سیاست دسترسی محدود به

داده‌ها و اقدامات فناوری مانند رمزگذاری، امضای دیجیتال و دریافت رمز به صورت پیامک، باید در عملیات یک محیط تجارت الکترونیکی و آنلاین، برای کنترل هر نوع جرایم سایبری مانند سرقت هویت، اعمال شود. قصد خرید مصرف‌کنندگان در یک محیط تجارت الکترونیکی اساساً به اثر مشترک عملکرد عملیاتی قابل اعتماد و ارزش قیمت محصولات/خدمات وابسته است.

با این حال، اثر قیمت در ازای ارزش دریافتی، تاثیر قابل توجه و معناداری در پیگیری یا جلوگیری از قصد خرید آنلاین یا آنلاینی ندارد. درحالی که کنترل جرایم سایبری از طریق اعمال این اقدامات می‌تواند باعث افزایش نگرش تمایل به اعتماد باشد اما به طور بالقوه می‌تواند درک مصرف‌کننده از عملکرد عملیاتی را کاهش دهد. با این وجود، تاثیر اعتماد درک شده در پیگیری قصد خرید آن قدر برجسته و زیاد است که تاثیر منفی عملکرد عملیاتی، می‌تواند به طور قابل توجهی جبران شود؛ بنابراین، با توجه به تاثیر همه جانبه این سه سازه، پس از اعمال اقدامات کنترلی در برابر سرقت هویت، قصد خرید و ادامه آن در یک محیط تجارت الکترونیکی یا آنلاینی یا آنلاینی مصرف‌کنندگان توصیه و تسريع می‌شود. همچنین اگر مصرف‌کنندگان، اعتماد بیشتری پیدا کنند، به خرید از یک محیط تجارت الکترونیکی یا آنلاینی ادامه خواهند داد.

لذا الزام به حفظ حریم خصوصی در مورد اشتراک گذاری اطلاعات شخصی به تدریج در حال افزایش است و اضطراب مصرف‌کنندگان به دلیل نامشخص بودن یک رسانه مجازی با توجه به ویژگی‌های آن بر توسعه نگرش تمایل به اعتماد تاثیر دارد؛ با این حال، برای توسعه اعتماد در یک رسانه مجازی مانند یک محیط تجارت الکترونیکی، درک امنیت در برابر هک وبسایت و سرقت اطلاعات مالی حساس، مهم ترین مساله و پارامتر است. اگر سایت آنلاینی یا یک محیط تجارت الکترونیکی، امن و بدون خطر در برابر هر نوع جرایم سایبری باشد، مصرف‌کنندگان اعتماد بیشتری به تجارت در یک محیط الکترونیکی یا آنلاینی خواهند داشت و این پیش بینی کننده غالب، برای پیگیری قصد خرید است. یافته‌ها همسو با مبانی و چارچوب‌های نظری از جمله نظریه یکپارچه پذیرش و استفاده از فناوری [29]، رویکرد هزینه معامله یا مبادله و نظریه مبادله اجتماعی [42] می‌باشد.

به این شرح که مصرف‌کنندگان رفتار خود را برای خرید آنلاین در صورتی که آن را مفید بدانند، تقویت می‌کنند؛ مصرف‌کنندگان همیشه نگران ارزش زمان و ارزش تلاش درک شده هستند که ممکن است از پذیرش هر سیستمی جلوگیری کند؛ اگر مصرف‌کنندگان برای معامله در یک محیط نامطمئن، احساس خطر کنند اما قصد خرید آن‌ها، به درک مصرف‌کنندگان از ارزش مبادله‌ای که دریافت می‌کنند، بستگی دارد، که با اعتماد و عملکرد عملیاتی مرتبط است. با این حال برخی از پدیده‌های منفی مانند تاخیر زمانی و تلاش بیشتر در عملیات تجارت در یک محیط الکترونیکی یا آنلاینی و قیمت کمی بالاتر محصول، می‌تواند مشتریان را از خرید آنلاین پس از به کارگیری مکانیزم‌های کنترلی پیچیده تکنولوژیکی و مدیریتی در مرحله مبادلات تجارت در محیط الکترونیکی باز دارد.

با این حال، این برنامه‌ها می‌توانند به طور قابل توجهی، اعتماد مصرف‌کنندگان را افزایش دهند. از آنجایی که استفاده از اقدامات سرقت هویت به طور بالقوه می‌تواند خطر از دست دادن اطلاعات مالی و در نتیجه تجربه بد یا وقوع از دست دادن پول در آینده را کاهش دهد، افزایش جزیی قیمت ممکن است مستقیماً مشتریان را در خرید از یک محیط تجارت الکترونیکی یا آنلاینی کند نکند. در نهایت علیرغم اینکه مطالعه حاضر سهم بالقوه‌ای برای شناخت و بررسی ابعاد مختلف عملیات در یک محیط تجارت الکترونیکی دارد اما در حد اكمل خود صورت نگرفته است؛ بنابراین محققان آینده می‌توانند این مهم را در بین کشورها، بین مصرف‌کنندگان و اقشار مختلف انجام دهند. همچنین تاثیر تعدیل کننده متغیرهای جمعیت شناختی مانند درآمد، جنسیت و سن را مورد بررسی قرار دهند.

منابع

- [1] Shareef, M. A., Mukerji, B., Alryalat, M. A. A., Wright, A., & Dwivedi, Y. K. (2018). Advertisements on facebook: Identifying the persuasive elements in the development of positive attitudes in consumers. *Journal of retailing and consumer services*, 43, 258–268. <https://doi.org/10.1016/j.jretconser.2018.04.006>
- [2] Dwivedi, Y. K., Shareef, M. A., Simintiras, A. C., Lal, B., & Weerakkody, V. (2016). A generalised adoption model for services: A cross-country comparison of mobile health (m-health). *Government information quarterly*, 33(1), 174–187. <https://doi.org/10.1016/j.giq.2015.06.003>
- [3] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International journal of human computer studies*, 59(4), 451–474. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- [4] Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2014). Rogers' innovation adoption attributes: A systematic review and synthesis of existing research. *Information systems management*, 31(1), 74–91. <https://doi.org/10.1080/10580530.2014.854103>

- [5] Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic commerce research and applications*, 10(6), 702–715. <https://doi.org/10.1016/j.elerap.2011.07.003>
- [6] Rana, N. P., Dwivedi, Y. K., Williams, M. D., & Weerakkody, V. (2016). Adoption of online public grievance redressal system in India: Toward developing a unified view. *Computers in human behavior*, 59, 265–282. <https://doi.org/10.1016/j.chb.2016.02.019>
- [7] Aïmeur, E., & Schönfeld, D. (2011). The ultimate invasion of privacy: identity theft. *2011 ninth annual international conference on privacy, security and trust* (pp. 24–31). IEEE. <https://doi.org/10.1109/PST.2011.5971959>
- [8] Saleh, Z. (2013). The impact of identity theft on perceived security and trusting E-commerce. *Journal of internet banking and commerce*, 18(2), 1–11. <https://B2n.ir/bd9305>
- [9] Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of services marketing*, 24(3), 219–229. <https://doi.org/10.1108/08876041011040622>
- [10] Shareef, M. A., Uma Kumar, & Vinod Kumar. (2019). Role of different electroniccommerce (EC) quality factors on purchase decision: a developing country perspective. *Journal of electronic commerce research*, 9(2), 92–113. <https://B2n.ir/hb6566>
- [11] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and tam in online shopping: AN integrated model. *MIS quarterly: management information systems*, 27(1), 51–90. <http://dx.doi.org/10.2307/30036519>
- [12] Razmak, J., & Bélanger, C. (2018). Using the technology acceptance model to predict patient attitude toward personal health records in regional communities. *Information technology and people*, 31(2), 306–326. <https://doi.org/10.1108/ITP-07-2016-0160>
- [13] Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of economic perspectives*, 22(2), 171–192. <https://www.scrip.org/reference/referencespapers?referenceid=2615528>
- [14] Douglass, D. B. (2009). An examination of the fraud liability shift in consumer card-based payment systems. *Economic perspectives*, 33(1), 43–49. <https://ssrn.com/abstract=1341696>
- [15] Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. (2014). Factors affecting citizen adoption of transactional electronic government. *Journal of enterprise information management*, 27(4), 385–401. <https://doi.org/10.1108/JEIM-12-2012-0084>
- [16] Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- [17] Hartmann-Wendels, T., Mählmann, T., & Versen, T. (2009). Determinants of banks' risk exposure to new account fraud - Evidence from Germany. *Journal of banking and finance*, 33(2), 347–357. <https://doi.org/10.1016/j.jbankfin.2008.08.005>
- [18] Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information systems research*, 24(3), 579–595. <https://doi.org/10.1287/isre.1120.0441>
- [19] Collier, J. E., & Bienstock, C. C. (2006). Measuring service quality in E-retailing. *Journal of service research*, 8(3), 260–275. <https://doi.org/10.1177/1094670505278867>
- [20] Shareef, M. A., Kumar, V., Dwivedi, Y. K., & Kumar, U. (2014). Global service quality of business-to-consumer electronic-commerce. *International journal of Indian culture and business management*, 8(1), 1–34. <https://doi.org/10.1504/IJICBM.2014.057947>
- [21] Shareef, M. A., & Kumar, V. (2012). Prevent/control identity theft: Impact on trust and consumers' purchase intention in B2C EC. *Information resources management journal (IRMJ)*, 25(3), 30–60. <https://www.igi-global.com/article/content/68426>
- [22] Cheng, X., Fu, S., Han, Y., & Zarifis, A. (2017). Investigating the individual trust and school performance in semi-virtual collaboration groups. *Information technology and people*, 30(3), 691–707. <https://doi.org/10.1108/ITP-01-2016-0024>
- [23] Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45(3), 285–297. <https://doi.org/10.1002/ejsp.2049>
- [24] Marilynn, B. B. (1999). The psychology of prejudice: Ingroup love and outgroup hate? *Journal of social issues*, 55(3), 429–444. <https://doi.org/10.1111/0022-4537.00126>
- [25] Gudykunst, W. B., & Nishida, T. (2001). Anxiety, uncertainty, and perceived effectiveness of communication across relationships and cultures. *International journal of intercultural relations*, 25(1), 55–71. [https://doi.org/10.1016/S0147-1767\(00\)00042-0](https://doi.org/10.1016/S0147-1767(00)00042-0)
- [26] Shareef, M. A., Kumar, U., Kumar, V., & Dwivedi, Y. K. (2009). Identifying critical factors for adoption of e-government. *Electronic government, an international journal*, 6(1), 70–96. <https://doi.org/10.1504/EG.2009.022594>
- [27] Alford, J. (2002). Defining the client in the public sector: A social-exchange perspective. *Public administration review*, 62(3), 337–346. <http://dx.doi.org/10.1111/1540-6210.00183>
- [28] Dodds, W. B., Monroe, K. B., & Grewal, D. (1991). Effects of Price, Brand, and Store Information on Buyers' Product Evaluations. *Journal of marketing research*, 28(3), 307. <http://dx.doi.org/10.2307/3172866>
- [29] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 36(1), 157–178. <http://dx.doi.org/10.2307/41410412>
- [30] Mansoori, K. A. Al, Sarabdeen, J., & Tchantchane, A. L. (2018). Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using modified UTAUT model. *Information technology and people*, 31(2), 455–481. <https://doi.org/10.1108/ITP-12-2016-0290>

- [31] Ali, S., Uppal, M. A., & Gulliver, S. R. (2018). A conceptual framework highlighting e-learning implementation barriers. *Information technology and people*, 31(1), 156–180. <https://doi.org/10.1108/ITP-10-2016-0246>
- [32] Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information systems journal*, 15(1), 5–25. <https://doi.org/10.1111/j.1365-2575.2005.00183.x>
- [33] Rogers, E. M. (1995). *Diffusion of Innovations*. (The Free Press: New York, NY, USA). The Free Press. <https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1786060>
- [34] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3), 319–340. <http://dx.doi.org/10.2307/249008>
- [35] Antonakis, J., Bendahan, S., Jacquart, P., Lalive, R., & others. (2014). Causality and endogeneity: Problems and solutions. *The oxford handbook of leadership and organizations*, 1(6), 93–117. <https://psycnet.apa.org/record/2014-16828-006>
- [36] Rubin, D. B. (2008). For objective causal inference, design trumps analysis. *Annals of applied statistics*, 2(3), 808–840. <http://dx.doi.org/10.1214/08-AOAS187>
- [37] Mulaik, S. A. (2009). *Linear causal modeling with structural equations*. Chapman and Hall/CRC. <https://doi.org/10.1201/9781439800393>
- [38] Chau, P. Y. K. (1997). Reexamining a model for evaluating information center success using a structural equation modeling approach. *Decision sciences*, 28(2), 309–334. <https://doi.org/10.1111/j.1540-5915.1997.tb01313.x>
- [39] Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford publications. <https://B2n.ir/mm2696>
- [40] Bauer, R. A. (1960). Consumer behavior as risk taking. *Dynamic marketing for a changing world, proceedings of the 43rd american marketing association conference* (pp. 389–398). Chicago, IL. <https://cir.nii.ac.jp/crid/1572543025452826496>
- [41] Burnham, T. A., Frels, J. K., & Mahajan, V. (2003). Consumer switching costs: A typology, antecedents, and consequences. *Journal of the academy of marketing science*, 31(2), 109–126. <https://doi.org/10.1177/0092070302250897>
- [42] Thibaut, J., & Kelley, H. (2008). Social exchange theory. In *A first look at communication theory* (Vol. 2, pp. 196–205). McGraw Hill New York, NY. http://dx.doi.org/10.1007/978-94-007-6772-0_3

