پژوهش‌های مدیریت عمومی
سال سیزدهم، شماره پنجاهم، زمستان ۱۳۹۹
صفحه ۲۰۴-۱۷۹

تاریخ دریافت : ۱۳۹۹/۰۶/۰۵
تاریخ پذیرش : ۱۳۹۹/۰۸/۲۸

The Effect of Security Awareness on Compliance with Security Regulations by Teleworkers in the Period of COVID-19 Epidemic

Mohammad Reza Taghva[1]

1-Associate Professor of Allameh Tabataba'i University, Tehran, Iran.
E-mail: taghva@atu.ac.ir

Received: 05/08/2020; Accepted: 19/10/2020

Extended abstract

Abstract

The aim of this research was to investigate the effect of security awareness on compliance with security regulations by teleworkers during the epidemic of COVID-19 using the Health Belief Model (HBM). Users who experienced teleworking in organizations in Tehran after the outbreak of the disease were selected as the statistical population of this study and 288 people completed the research questionnaire and participated in it. The samples were selected using the available sampling method and then the information and research hypotheses were analyzed using structural equation modeling. The research findings showed that security awareness does not directly affect the compliance with security regulations in organizations by teleworking personnel, but it affects their privacy concerns and security expectations, and these two elements can lead them to more adhering to security regulations and policies of organizations.

Introduction

Covid-19 pandemic is considered to be the most important global health disaster of the century and is the greatest challenge facing humanity since World War II. In fact, the corona outbreak is an example of a widespread crisis; A crisis in which events or their sequences occur on a large scale and are of astonishing speed, leading to a high degree of uncertainty that exacerbates irregularities. It creates a feeling of lack of control and causes emotional disturbance in people.

This study attempts to examine the issue of security awareness and compliance with security regulations by employees, using the health belief model. Hochbaum (1958) developed the health belief model to study the behavior of

individuals in health research. Based on what has been stated, the purpose of this study is to investigate whether users involved in telecworking have security awareness and whether there is a relationship between this security awareness and users' compliance with security regulations.

Theoretical framework

The health belief model was developed in the 1950s to explain and predict preventive health behaviors. This model identifies the feasibility, benefits, and costs associated with behavior intervention or change based on the four constructs (sensitivity, severity, benefits, and perceived barriers). In the field of information systems, this model can be used to explain the security behavior of users. This study uses the health belief model as the basis of its research model. The model includes constructs of perceived severity, perceived sensitivity, perceived threat, expectations (perceived benefits and barriers), and cues of action. In addition, the proposed model of the present study includes three other structures that do not exist in the health belief model: security awareness, privacy concern, and compliance with security regulations.

Methodology

The approach of this study to achieve the results is to use a quantitative method with the data collected through a questionnaire and a survey. The questionnaire assesses security awareness, information privacy concerns, self-efficacy, expectations of security measures, security threats, and participants' security behavior. The statistical population of this study consists of people involved in teleworking in Iranian organizations. The questionnaire consists of two parts: general questions (gender, job title, passing security courses in the organization and the level of proficiency in using common IT tools) and specialized questions that are categorized based on the components of the research. Specialized questions consist of four parts; health belief model, privacy concern, security compliance, and security awareness. To test the hypotheses of this study, structural equation modeling and multiple regression analysis were used.

Discussion and results

According to the results obtained from the test of research hypotheses, it was found that all research hypotheses were confirmed and only hypothesis 9 (the effect of perceived threat on compliance with security regulations) was not approved. These results mean that security awareness has a positive effect on expectations (perceived benefits - perceived barriers), privacy concerns, and perceived threats. These results are consistent with the results of previous studies. In addition, the results showed that the severity and sensitivity perceived by users has a positive effect on the perceived threat by them. These results are consistent with the results of previous studies. Expectations and

privacy concerns also have a positive and significant effect on compliance with security regulations. These results are completely consistent with the results obtained in the past. In another part of the research results, it was found that privacy concerns and cues of action have a positive and significant effect on perceived threat. These results are fully consistent with studies conducted other researchers. However, the results of the study indicate that perceived threats to security issues do not have a significant effect on compliance with security regulations.

Conclusion

In summary, the findings of this study show that the majority of teleworking users are somewhat aware of security issues (especially in the field of social engineering). Although this issue does not directly affect compliance with organizations' security regulations and policies, it does affect expectations, privacy concerns, and perceived threats. Also, expectations and privacy concerns have a positive and significant effect on compliance with security regulations in organizations, but the perceived threat has no significant effect on compliance with these regulations. Based on the above results, the managers of organizations (especially information technology and security managers) can be advised to improve their staff awareness of security issues related to teleworking by holding awareness and training courses in the field of information security. Consequently, in the case of incidents and events (such as the outbreak of Covid-19 pandemic) that inevitably lead to teleworking, they can comply with the organization's security regulations in their organizational activities so as not to compromise the organization's data and information.

Keywords: Security Awareness, Covid-19, Health Belief Model, Security Regulations.

تاثیر آگاهی امنیتی بر پیروی از مقررات امنیتی از سوی کاربران دورکاری در دوره همه‌گیری بیماری کووید-۱۹

دکتر محمدرضا تقوا*

چکیده

هدف از پژوهش حاضر، بررسی تاثیر آگاهی امنیتی بر پیروی از مقررات امنیتی از سوی کاربران دورکاری در دوره همه‌گیری بیماری کووید-۱۹ با استفاده مدل باور سلامتی (HBM) است. کاربرانی که پس از همه‌گیری این بیماری، تجربه دورکاری در سازمان‌ها در شهر تهران داشتند، به عنوان جامعه آماری این پژوهش انتخاب شدند و ۲۸۸ نفر، پرسشنامه پژوهش را تکمیل و در آن مشارکت کردند. نمونه‌ها با استفاده از روش نمونه‌گیری در دسترس انتخاب شدند و سپس اطلاعات و فرضیه‌های پژوهش با استفاده از روش مدل‌سازی معادلات ساختاری مورد تحلیل و آزمون قرار گرفتند. یافته‌های پژوهش نشان دادند که آگاهی امنیتی به طور مستقیم بر پیروی از مقررات امنیتی در سازمان‌ها توسط پرسنل دورکار تاثیر ندارد، اما بر نگرانی حریم خصوصی و انتظارات امنیتی آن‌ها اثرگذار است و این دو مورد می‌توانند منتهی به تبعیت بیشتر پرسنل دورکار از مقررات و سیاست‌های امنیتی در سازمان‌ها شود.

واژه‌های کلیدی : آگاهی امنیتی، کووید-۱۹، مدل باور سلامتی، مقررات امنیتی.

* دانشیار گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران.
taghva@atu.ac.ir

مقدمه

پس از ثبت اولین گزارش‌ها از شیوع ویروس کرونا (کووید-۱۹[1]) به مرکزیت ووهان چین، این بیماری به سرعت در بیش از صد کشور به صورت بحرانی گسترش پیدا کرد (*Payande, Majdizade & Mirzapour, 2020*). این ویروس همچنان در جهان گسترش پیدا می‌کند و پیامدهایی جدی را برای اقتصاد کشورها و کسب‌وکارهای کوچک و بزرگ به وجود می‌آورد (*Nasri, Bagheri & Boushehri, 2020*).

بیماری همه‌گیر کووید-۱۹ به عنوان مهم‌ترین بلای جهانی سلامت در قرن حاضر محسوب شده و بزرگ‌ترین چالشی است که بشریت از زمان جنگ جهانی دوم با آن مواجه است. در حقیقت شیوع کرونا یک نمونه کامل از یک بحران گسترده است؛ بحرانی که در آن رویدادها یا توالی آن‌ها در مقیاس‌های بزرگی رخ می‌دهد، سرعت خیره‌کننده‌ای دارد و این امر منجر به درجه بالایی از عدم قطعیت می‌شود که بی‌نظمی‌ها را شدت می‌بخشد، احساس فقدان کنترل را به وجود می‌آورد و در افراد اختلال عاطفی ایجاد می‌کند (*Mirnezami & Rajabi, 2020*).

به منظور محدود کردن انتقال بیشتر این بیماری در جامعه، بسیاری از کشورهای درگیر، تصمیم به قرنطینه و تعطیلی کامل کسب‌وکارها گرفتند (*Chakraborty & Maity, 2020*). با توجه به لزوم به حداقل رساندن حضور فیزیکی افراد در محل کار، بسیاری از سازمان‌ها به روش‌های جایگزین کار حضوری از جمله دورکاری[2] روی آوردند. علی‌رغم مزایای بسیار این شیوه، مخاطرات پیرامون امنیت اطلاعات برای بسیاری از سازمان‌ها تبدیل به چالش بزرگی بر سر راه به‌کارگیری دورکاری شده است.

حملات به سیستم‌های کامپیوتری، همچنان یک مسئله جدی است. حملات بدافزار و فیشینگ[3] سالانه میلیون‌ها کاربر را تحت‌تاثیر قرار می‌دهد و کسب‌وکارها و مصرف‌کنندگان متحمل میلیاردها دلار هزینه می‌شوند (*Anti-Phishing Workgroup, 2015*). کاربران باید از این حملات آگاه باشند و بیاموزند چطور از خود در برابر این حملات محافظت کنند

1-COVID-19
2-Teleworking
3-Phishing

(Kritzinger & von Solms, 2010). بنابراین آگاهی امنیتی کاربران نقش بسزایی در امنیت اطلاعات سازمان در این نوع کار دارد.

با این وجود، بسیاری از نقض‌های امنیت اطلاعات حین کار، ناشی از عدم پیروی کارکنان از سیاست‌های امنیت اطلاعات سازمان‌ها است. اشتباه‌ها، خطاها، عادات نامناسب و عدم آگاهی افراد می‌تواند موجب به خطر افتادن امنیت اطلاعات در سازمان گردد؛ بنابراین باید به این نکته توجه کرد که پیروی کارکنان، مهم‌ترین عامل در امنیت سیستم‌های اطلاعاتی در سازمان است (Jafari, Hamidizadeh & Montazeri Najafabadi, 2016) و لذا درک میزان پیروی کارکنان از سیاست‌های امنیتی برای سازمان‌ها بسیار حیاتی است (Bulgurcu, Cavusoglu & Benbasat, 2010).

این پژوهش تلاش می‌کند تا موضوع آگاهی امنیتی و پیروی از مقررات امنیتی توسط کارکنان را با استفاده از مدل باور سلامتی[1] بررسی کند. هوکبام (Hochbaum, 1958) مدل باور سلامتی را برای مطالعه رفتار افراد در پژوهش‌های مربوط به سلامت توسعه داد. این مدل بر اساس مدل‌های روان‌شناختی و رفتاری فرض می‌کند که رفتار یک فرد به ارزشی که وی برای یک هدف خاص قائل است و احتمال دستیابی به آن هدف با انجام یک عمل مشخص بستگی دارد (Janz & Becker, 1984).

علاوه بر روشن نبودن میزان آگاهی امنیتی کاربران درگیر دورکاری، اینکه چه بخشی از آگاهی امنیتی در انگیزه دادن به کاربران در پیروی از مقررات امنیتی نقش دارد نیز روشن نیست. اگرچه کاربران تا حدی با مفاهیم آگاهی امنیتی آشنایی دارند (Cone, Irvine., Thompson & Nguyen, 2007; Kruger & Kearney, 2006)، اما هنوز خود را با رفتار ناامن در معرض خطر قرار می‌دهند (Rhee, Kim, & Ryu, 2009; Styles & Tryfonas, 2009).

بر اساس آنچه بیان شد، هدف این پژوهش بررسی این موضوع است که آیا کاربران درگیر دورکاری، آگاهی امنیتی دارند و آیا رابطه‌ای میان این آگاهی امنیتی و پیروی از مقررات امنیتی توسط کاربران وجود دارد. در بخش‌های بعدی به پیشینه تحقیقات انجام‌شده در

1-Health Belief Model (HBM)

زمینه پژوهش حاضر پرداخته و در ادامه، روش تحقیق، تحلیل یافته‌ها، نتایج و پیشنهادها بیان می‌شود.

پیشینه پژوهش

با توجه به هدف این پژوهش که بررسی رابطه بین آگاهی امنیتی و پیروی از مقررات امنیتی توسط کاربران درگیر دورکاری است، در این بخش به بررسی پیشینه پژوهش‌های انجام‌گرفته در این حوزه پرداخته می‌شود. این مطالعه مدل باور سلامتی را به عنوان اساس مدل تحقیقاتی خود مورد استفاده قرار داده است. این مدل شامل سازه‌های شدت درک شده، حساسیت درک شده، تهدید درک شده، انتظارات (مزایا و موانع درک شده) و نشانه‌های عمل است. علاوه بر این، مدل پیشنهادی پژوهش حاضر شامل سه سازه دیگر است که در مدل باور سلامتی وجود ندارند: آگاهی امنیتی، نگرانی حفظ حریم خصوصی و پیروی از مقررات امنیتی.

مدل باور سلامتی در دهه ۱۹۵۰ برای توضیح و پیش‌بینی رفتارهای بهداشتی پیشگیرانه توسعه داده شد (*Ross, Ross, Rahman & Cataldo, 2010*). این مدل امکان‌پذیری، مزایا و هزینه‌های مربوط به مداخله یا تغییر رفتار را بر اساس چهار سازه حساسیت، شدت، مزایا و موانع درک شده مشخص می‌کند. در حوزه سیستم‌های اطلاعاتی می‌توان این مدل را برای توضیح رفتار امنیتی کاربران به کار گرفت.

در مدل باور سلامتی، حساسیت درک‌شده باوری است که یک فرد در مورد خطر ابتلا به یک بیماری دارد (*Glanz, Rimer & Viswanath, 2008*). شدت درک‌شده، دیدگاه فرد درباره جدی بودن بیماری و پیامدهای بالینی و/یا اجتماعی ابتلا به بیماری است (*Glanz et al., 2008*). در این مطالعه، حساسیت درک‌شده به معنای باور یک فرد درباره آسیب‌پذیری در برابر تهدید امنیتی کامپیوتری و شدت درک‌شده، به معنای باور وی درباره میزان تاثیرپذیری از تهدید امنیتی کامپیوتری است. تهدید درک شده روی قصد فرد برای انجام یک رفتار مربوط به سلامتی تاثیر می‌گذارد. تهدید امنیتی درک شده "میزانی است که یک فرد فناوری اطلاعات را مخاطره‌آمیز یا مضر می‌داند" (*Liang & Xue, 2010, 397*). این سازه ترکیبی از حساسیت و شدت درک شده است. لیانگ و ژو (۲۰۱۰) نشان دادند که ترکیب سازه‌های حساسیت و شدت درک شده به طور مثبت بر سازه تهدید درک‌شده اثر

دارند. مزایای درک‌شده، شامل دیدگاه فرد درباره تاثیر یک رفتار در کاهش شانس ابتلا به یک بیماری و یا حذف بیماری حاضر است (*Hayden, 2009*). در این مطالعه، مزایای درک‌شده، باور به کارایی یک اقدام برای کاهش یا حذف یک تهدید امنیتی است. موانع درک‌شده موانعی هستند که یک فرد آن‌ها را به عنوان مانعی برای اقدام می‌داند. جانز و بکر (۱۹۸۴) موانع درک‌شده را به عنوان مهم‌ترین سازه برای تعیین تغییر رفتاری در نظر می‌گیرند. در این مطالعه، موانع درک شده به عنوان موانعی تعریف می‌شوند که روی تصمیم فرد برای یک اقدام امنیتی معین تاثیر منفی می‌گذارند. نشانه‌های عمل، رویدادهایی هستند که به مردم انگیزه می‌دهند تا رفتار خود را تغییر دهند (*Hayden, 2009*). هوکبام (۱۹۵۸) اظهار داشت که نشانه‌های عمل می‌توانند تغییرات فیزیکی در بدن یک فرد، گزارش‌های رسانه‌ها، مقالات در مورد یک بیماری، شناختن کسی که بیماری دارد، و یا توصیه از طرف یک فرد قابل‌اعتماد باشد. در این مطالعه، نشانه‌های عمل، تجربه قبلی فرد در مواجهه با مسائل امنیتی، گزارش‌های رسانه‌ای درباره امنیت کامپیوتری، مقالات امنیتی و اطلاعات از یک منبع مورد اعتماد هستند. هایدن (۲۰۰۹) و جانز و بکر (۱۹۸۴) نشان دادند که سازه نشانه‌های عمل به طور مثبت بر سازه تهدید درک‌شده اثر دارد.

کاربرانی که نگران حریم خصوصی خود هستند، بر این باورند که شرکت‌های آنلاین تمایل به سوءاستفاده از اطلاعات شخصی مشتریان دارند (*Dinev & Hart, 2005; Van Slyke, Shin, Johnson & Jiang, 2006*). نگرانی افراد برای حفظ حریم خصوصی بر تصمیم آن‌ها در ذخیره‌سازی اطلاعات خود در رسانه‌های الکترونیکی تاثیر می‌گذارد (*Angst & Agarwal, 2009; Dinev & Hart, 2005*). وان اسلایک و همکاران (۲۰۰۶) و چو (*Cho, Rivera & Lim, 2009*) نشان دادند که سازه نگرانی برای حفظ حریم خصوصی به طور مثبت بر سازه تهدید درک‌شده اثر دارد.

آگاهی امنیتی می‌تواند به عنوان برخورداری از دانش درباره روش‌های امنیتی مناسب و دانستن اهمیت محافظت از داده‌های شخصی/ سازمانی موجود در کامپیوترهایی که کاربر به آن‌ها دسترسی دارد، تعریف شود. سازه آگاهی امنیتی به طور مثبت بر سازه مزایا و موانع درک شده اثر دارد. الابری و همکاران (*Al Abri, McGill & Dixon, 2009*) و دینو و هارت (۲۰۰۵) نشان دادند که این سازه روی سازه نگرانی برای حفظ حریم خصوصی هم تاثیر

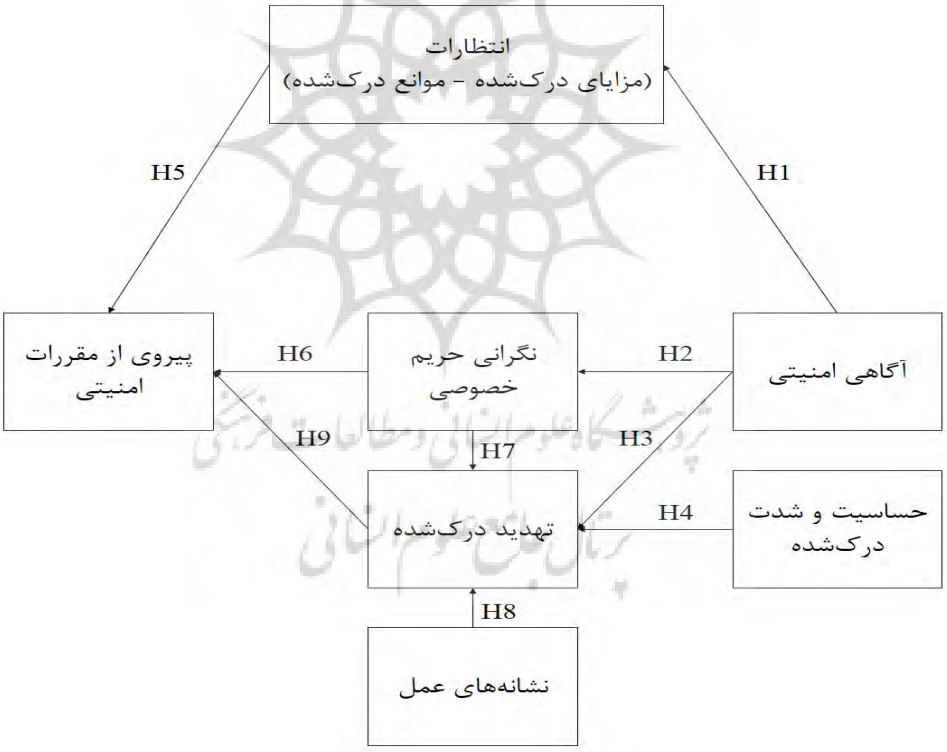
مثبت دارد. دارسی و همکاران (D'Arcy, Hovav & Galletta, 2009) نشان دادند که سازه آگاهی امنیتی به طور مثبت بر سازه تهدید درک‌شده نیز اثر دارد.

بولگورجو و همکاران (۲۰۱۰) ذکر می‌کنند که جهت‌گیری اصلی در پژوهش‌های عوامل انسانی در رابطه با امنیت اطلاعات، پیدا کردن عواملی است که مرتبط با رفتار کارکنان و پیروی آن‌ها از سیاست‌های امنیت اطلاعات در سازمان است. منظور از تمایل به پیروی از سیاست‌های امنیت اطلاعات، قصد کارکنان برای حفاظت از منابع فناوری و اطلاعات سازمان خویش در برابر نقض بالقوه امنیت است (Bulgurcu et al., 2010; Ajzen, 1991; Fishbein & Ajzen, 1975). هومیدی و همکاران (Humaidi, Balakrishnan & Shahrom, 2014) نشان دادند که سازه‌های مزایا و موانع درک‌شده بر سازه پیروی از مقررات امنیتی اثر دارند. چو (۲۰۱۰) نشان داد که نگرانی برای حفظ حریم خصوصی باعث رفتار خودمحافظتی فرد می‌شود. این رفتار باعث می‌شود فرد به شیوه خود عمل کرده و در نتیجه از از مقررات و رویه‌های امنیتی سازمان پیروی نکند. پس می‌توان فرض کرد که سازه نگرانی برای حفظ حریم خصوصی به طور منفی بر سازه پیروی از مقررات امنیتی اثر دارد. کلار (Claar, 2011) و انجی و همکاران (Ng, Kankanhalli & Xu, 2009) نشان دادند که سازه تهدید درک‌شده به طور مثبت بر سازه رفتار امنیتی اثر دارد. از آنجا که پیروی از مقررات امنیتی نیز نوعی رفتار امنیتی تلقی می‌شود، پس می‌توان فرض کرد سازه تهدید درک‌شده، تاثیر مثبتی بر سازه پیروی از مقررات امنیتی دارد.

کولوسنی و همکاران (۲۰۱۹) در پژوهش خود، رفتارهای امنیتی کارکنان را با استفاده از مدل باور سلامتی بررسی کردند. آن‌ها این مدل را برای مطالعه رفتارهای امنیتی مرسوم (عادت‌های امنیتی) و رفتارهای امنیتی آگاهانه در میان کارکنان دولت تانزانیا به کار گرفتند و با استفاده از مدلسازی معادلات ساختاری دریافتند که قصد کارکنان در رفتارهای امنیتی تحت تاثیر شدت، حساسیت و موانع درک‌شده، نشانه‌های عمل و عادت‌های امنیتی است، اما متاثر از مزایای درک‌شده نیست. هومیدی و همکاران (۲۰۱۴) در مطالعه‌ای دیگر و با استفاده از مدل باور سلامتی، تاثیر عوامل آگاهی امنیتی بر رفتارهای انطباقی کاربران در حوزه سیاست‌های امنیتی سیستم‌های اطلاعات سلامت را بررسی کردند و به این نتیجه رسیدند که شدت، مزایا و موانع درک‌شده، نشانه‌های عمل و تجربه کاری، توانایی

پیش‌بینی رفتار منطبق با سیاست‌های امنیتی سیستم‌های اطلاعات سلامت را دارند، در حالی که حساسیت درک‌شده چنین توانایی را ندارد. انجی و همکاران (۲۰۰۹) نیز با استفاده از مدل باور سلامتی، رفتارهای امنیتی کاربران را سنجیدند و نشان دادند که حساسیت و مزایای درک‌شده، عوامل تعیین‌کننده رفتارهای امنیتی کاربران پیرامون ایمیل هستند و شدت درک‌شده نیز دارای اثر میانجی‌گری در ارتباط بین مزایای درک‌شده، جهت‌گیری امنیتی و نشانه‌های عمل با رفتار امنیتی است.

با توجه به تعاریف بیان شده و بنا بر مجموعه پژوهش‌های پیشین، در این پژوهش مدل مفهومی مطابق با شکل ۱ برای بررسی رابطه میان آگاهی امنیتی و پیروی از مقررات امنیتی توسط کاربران درگیر دورکاری در سازمان‌ها ارائه شده است.



شکل ۱: مدل مفهومی پژوهش

روش‌شناسی پژوهش

رویکرد این مطالعه برای رسیدن به نتایج، استفاده از روش کمی با داده‌های جمع‌آوری‌شده از طریق پرسشنامه و به صورت پیمایشی است. این پرسشنامه آگاهی امنیتی، نگرانی‌های حفظ حریم خصوصی اطلاعات، خودکارآمدی، انتظارات از اقدامات امنیتی، تهدیدات امنیتی، و رفتار امنیتی شرکت‌کنندگان را ارزیابی می‌کند. جامعه آماری این مطالعه از افراد درگیر دورکاری در سازمان‌های ایران تشکیل شده است. کلیه شرکت‌کنندگان یک رایانه شخصی داشته و به طور منظم به اینترنت دسترسی دارند.

در این مطالعه از برنامه SPSS SamplePower برای محاسبه تعداد شرکت‌کنندگان مورد نیاز استفاده شده است. ورودی‌های مورد نیاز برای این کار عبارتند از: تعداد متغیرها، مقدار R2 و توان مشاهده‌شده. مطابق با گفته کوهن *(Cohen, 1988)*، مقدار R2 متوسط ۰,۱۳ استفاده می‌شود. روای، بیکر و پونتن *(Rovai, Baker & Ponton, 2014)*، استفاده از توان مشاهده‌شده ۸۰.۰ یا بالاتر را پیشنهاد می‌کنند، بنابراین توان مشاهده‌شده ۹۰.۰ در نظر گرفته شده است. با توجه به موارد مذکور، حداقل تعداد شرکت‌کنندگان مورد نیاز ۲۷۱ محاسبه شد. پرسشنامه‌ها از طریق ابزار و فرم طراحی پرسشنامه گوگل توزیع و جمع‌آوری شدند و ۲۸۸ نفر به پرسش‌ها پاسخ دادند که بیش از حداقل تعداد شرکت‌کنندگان مورد نیاز بود و برای انجام تحلیل کفایت می‌کرد. از آنجا که ثبت پاسخ به پرسشنامه مستلزم پاسخگویی به تمامی سوالات بود، هیچ داده ازدست‌رفته‌ای نیز وجود نداشت.

پرسشنامه‌ای که توسط محقق توسعه یافته، شامل ۵۱ سوال است. برای هر پرسش از یک مقیاس لیکرت ۴ یا ۵ امتیازی استفاده می‌شود. پرسشنامه شامل دو بخش سؤالات عمومی (جنسیت، عنوان شغلی، گذراندن دوره‌های امنیتی در سازمان و میزان مهارت در استفاده از ابزارهای معمول فناوری اطلاعات) سؤالات تخصصی است که بر اساس مؤلفه‌های مورد نظر پژوهش دسته‌بندی شده‌اند. از شرکت‌کنندگان پرسیده شد که تا چه اندازه در استفاده از ایمیل، رسانه‌های اجتماعی، واژه‌پردازها، خرید آنلاین، بانکداری آنلاین و زبان‌های برنامه‌نویسی مهارت دارند. هنگامی که به دنبال نگرش‌های شرکت‌کنندگان در نظرسنجی هستیم، مقیاس لیکرت به خوبی عمل می‌کند *(Nardi, 2003; Rea & Parker, 2005)*. سایر محققان نیز در تحقیقات امنیتی خود برای ثبت نگرش‌ها و باورهای شرکت‌کنندگان از

مقیاس لیکرت استفاده کرده‌اند (*Claar, 2011; Grant, 2010; Ng et al., 2009*). بنابراین برای سوالات مربوط به ابزارهای فوق از یک مقیاس لیکرت چهار گزینه‌ای استفاده شد. بقیه پرسشنامه از چهار قسمت تشکیل شده است؛ مدل باور سلامتی، نگرانی برای حفظ حریم خصوصی، پیروی از مقررات امنیتی و آگاهی امنیتی. برای ثبت باورهای شرکت‌کنندگان در این قسمت‌ها نیز از یک مقیاس لیکرت پنج گزینه‌ای استفاده شد. ابزارهای پرسشنامه باید به طور دقیق سازه‌های مورد مطالعه را بسنجند. موارد انتخابی برای ابزار پرسشنامه و روش بیان این موارد می‌تواند اثری منفی روی سنجش سازه‌ها داشته باشد. استراوب (*Straub, 1989*) پیشنهاد می‌کند که هر زمان که ممکن است، از پرسشنامه‌های مطالعات قبلی استفاده شود. بنابراین، اکثریت سوالات این پرسشنامه از پرسشنامه‌های موجود در مطالعات قبلی اقتباس شده‌اند. برای تحلیل داده‌های حاصل از پرسشنامه نیز نرم‌افزارهای SPSS و LISREL مورد استفاده قرار گرفتند. خلاصه نتایج حاصل‌شده پیرامون ویژگی‌های جمعیت‌شناختی مشارکت‌کنندگان این مطالعه در جدول ۱ آمده است.

جدول ۱: فراوانی و درصد فراوانی اطلاعات جمعیت شناختی و عمومی

ویژگی‌های جمعیت‌شناختی یا عمومی	دسته	فراوانی	درصد فراوانی
جنس	زن	۱۲۴	۴۳,۱
	مرد	۱۶۴	۵۶,۹
عنوان شغلی	کارشناس	۲۲۰	۷۶,۴
	مدیر	۴۴	۱۵,۳
	مدرس	۲۴	۸,۳
گذراندن دوره امنیتی در سازمان	بله	۱۰۰	۳۴,۷
	خیر	۱۸۸	۶۵,۳
ایمیل	اصلا	۱۲	۴,۲
	کم	۶۸	۲۳,۶
	متوسط	۱۰۰	۳۴,۷
	زیاد	۱۰۸	۳۷,۵
رسانه‌های اجتماعی	اصلا	۰	۰
	کم	۲۴	۸,۳
	متوسط	۱۱۶	۴۰,۳
	زیاد	۱۴۸	۵۱,۴

ویژگی‌های جمعیت‌شناختی یا عمومی	دسته	فراوانی	درصد فراوانی
واژه‌پردازها	اصلا	۱۲	۴,۲
	کم	۲۸	۹,۷
	متوسط	۸۰	۲۷,۸
	زیاد	۱۶۸	۵۸,۳
خرید آنلاین	اصلا	۱۶	۵,۶
	کم	۱۱۲	۳۸,۹
	متوسط	۱۲۰	۴۱,۷
	زیاد	۴۰	۱۳,۹
بانکداری آنلاین	اصلا	۲۰	۶,۹
	کم	۳۶	۱۲,۵
	متوسط	۱۲۰	۴۱,۷
	زیاد	۱۱۲	۳۸,۹
زبان‌های برنامه‌نویسی	اصلا	۱۰۸	۳۷,۵
	کم	۷۲	۲۵,۰
	متوسط	۴۴	۱۵,۳
	زیاد	۶۴	۲۲,۲

بر اساس نتایج نشان داده‌شده در جدول ۱، مشارکت‌کنندگان مرد (۵۶,۹ درصد) بیشتر از مشارکت‌کنندگان زن (۴۳,۱) بودند. مشاغل رده کارشناسی با ۷۶,۴ درصد، بیشترین میزان شرکت‌کنندگان در مطالعه را به خود اختصاص دادند و مدرسان نیز با ۸,۳ درصد، کمترین حضور را دارند. هم‌چنین ۶۵,۳ درصد از مشارکت‌کنندگان تاکنون هیچ دوره امنیتی در سازمان خود نگذرانده‌اند و تنها ۳۴,۷ درصد این افراد در چنین دوره‌هایی شرکت داشته‌اند. در حوزه مهارت در استفاده از ابزارهای معمول فناوری اطلاعات نیز به طور میانگین، غالب افراد شرکت‌کننده دارای مهارت زیاد در این حوزه‌ها بودند و درصد کمی از افراد نیز هیچ مهارتی در استفاده از این ابزارها نداشتند.

مدل‌سازی معادلات ساختاری (SEM)[1] یک تکنیک تحلیل چندمتغیری بسیار کلی و قوی از خانواده رگرسیون چندمتغیری که به پژوهشگر امکان این را می‌دهد که مجموعه ای از

1-Structural Equation Modeling

معادلات رگرسیون را به صورت همزمان مورد آزمون قرار دهند. جهت آزمودن فرضیه‌های این پژوهش، مدل‌سازی معادلات ساختاری و تحلیل رگرسیون چندگانه مورد استفاده قرار گرفت (*Gay, Mills & Airasian, 2009; Rovai et al., 2014; Weiers, 2002*). بررسی و تحلیل مدل‌های اندازه‌گیری در مراحل اولیه مطالعات تاییدی مفید است، چراکه می تواند روشنگر نقاط ضعف نظری بوده و به تفسیر یافته های پژوهش کمک نموده و در طرح مطالعات آینده سهم عمده ای داشته باشد؛ بر این اساس مدل سازی معادلات ساختاری شامل دو مرحله عمده تدوین مدل و آزمون مدل می باشد. در تدوین مدل محقق با استفاده از کلیه نظریات مرتبط، پژوهش و اطلاعات در دسترس به طرح مدل می پردازد و در این مرحله مدل روابط علی بین متغیرها را توصیف می‌نماید. ارتباط بین متغیرها می‌تواند مبین فرضیه‌هایی باشد که روابط علی بین متغیرهای مشهود و مکنون را از فضای تئوریک استنتاج کرده‌اند. مرحله بعدی، آزمون برازندگی و میزان انطباق این نظریه‌ها با داده‌های تجربی است که از جامعه معین گردآوری شده‌اند.

سازه‌های مورد بررسی در این مطالعه که شامل شدت درک‌شده، حساسیت درک‌شده، تهدید درک‌شده، انتظارات (مزایای درک‌شده – موانع درک‌شده)، نشانه‌های عمل، نگران حریم خصوصی، پیروی از مقررات امنیتی و آگاهی امنیتی در یک مدل اندازه‌گیری جداگانه مورد تجزیه و تحلیل قرار گرفتند. برای تایید هر یک از این مدل‌های اندازه‌گیری، سوالاتی که بار عاملی کمتر از ۰,۵ داشتند، باید حذف می‌شدند؛ اگرچه همان‌طور که در جدول ۲ قابل مشاهده است، هیچ‌یک از سوالات پژوهش چنین شرایطی را نداشتند و بنابراین همگی باقی ماندند.

جدول ۲: بار عاملی و ضرایب پایایی متغیرهای پژوهش

سازه	سوال	بار عاملی	آلفای کرونباخ	پایایی مرکب (CR)	متوسط واریانس استخراج‌شده (AVE)
شدت و حساسیت درک شده	Q9	۰/۹۶	۰/۹۳۶	۰/۹۷۱	۰/۶۳۲
	Q10	۰/۹۶			
	Q11	۰/۹۴			
	Q12	۰/۸۶			
	Q13	۰/۶۸			
	Q14	۰/۶۰			
	Q15	۰/۶۷			
	Q16	۰/۵۷			

سازه	سوال	بار عاملی	آلفای کرونباخ	پایایی مرکب (CR)	متوسط واریانس استخراج‌شده (AVE)
تهدید درک شده	Q17	۰/۸۸	۰/۸۸۹	۰/۹۱۹	۰/۶۴۹
	Q18	۰/۹۴			
	Q19	۰/۷۱			
	Q20	۰/۶۶			
انتظارات	Q21	۰/۶۹	۰/۷۹۱	۰/۸۴۳	۰/۵۱۷
	Q22	۰/۸۵			
	Q23	۰/۸۵			
	Q24	۰/۹۱			
	Q25	۰/۶۶			
	Q26	۰/۵۴			
	Q27	۰/۶۰			
	Q28	۰/۵۵			
نشانه‌های عمل	Q29	۰/۷۷	۰/۷۷۶	۰/۸۲۱	۰/۵۳۷
	Q30	۰/۷۲			
	Q31	۰/۷۰			
	Q32	۰/۷۴			
نگران حریم خصوصی	Q33	۰/۸۶	۰/۹۱۵	۰/۸۳۹	۰/۷۴۳
	Q34	۰/۷۱			
	Q35	۰/۹۱			
	Q36	۰/۹۵			
پیروی از مقررات امنیتی	Q37	۰/۸۷	۰/۹۲۰	۰/۹۵۱	۰/۵۶۱
	Q38	۰/۸۱			
	Q39	۰/۸۳			
	Q40	۰/۸۷			
	Q41	۰/۵۸			
	Q42	۰/۶۳			
	Q43	۰/۶۷			
	Q44	۰/۶۷			
آگاهی امنیتی	Q45	۰/۶۵	۰/۸۷۷	۰/۹۰۸	۰/۶۶۰
	Q46	۰/۸۶			
	Q47	۰/۸۸			
	Q48	۰/۷۷			
	Q49	۰/۸۰			
	Q50	۰/۸۹			

ارزیابی پایایی

هنگامی که محققان از سوالاتی با مقیاس لیکرت در پرسشنامه استفاده می‌کنند، آلفای کرونباخ یک انتخاب مناسب برای تعیین پایایی است؛ بنابراین پایایی متغیرهای این مطالعه نیز با استفاده از آلفای کرونباخ ارزیابی شد (*Gay et al., 2009; Trochim & Donnelly, 2008*). هم‌چنین دو متغیر پایایی مرکب (CR) و متوسط واریانس استخراج‌شده (AVE) نیز برای سنجش پایایی این پژوهش به کار گرفته شدند. به گفته باگازی و ئی (*Bagozzi & Yi, 1988*)، مقدار پایایی مرکب باید مساوی یا بیش از ۰,۶، متوسط واریانس استخراج‌شده مساوی یا بیش از ۰,۵ و آلفای کرونباخ نیز مساوی یا بیش از ۰,۷ باشد. همان‌طور که در جدول ۲ مشاهده شد، کلیه این مقادیر برای تمامی متغیرها در سطح پذیرفته‌شده جای دارند و لذا می‌توان نتیجه گرفت که پایایی مدل‌های اندازه‌گیری و متغیرهای پژوهش قابل قبول است.

ارزیابی روایی

برای ارزیابی روایی پژوهش، دو روش روایی محتوا (*Straub, Boudreau & Gefen, 2004*) و روایی سازه (روایی همگرا و روایی واگرا) مورد استفاده قرار گرفت. روایی محتوا به میزانی که یک سازه به اندازه کافی شامل تمام اطلاعات مربوطه باشد، اشاره دارد (*Ghauri, gronhaug & strange, 2020*). روایی محتوا می‌تواند با استفاده از سوالاتی که در مطالعات قبلی استفاده شده و روایی آن‌ها ثابت شده است و نیز با استفاده از نظرات خبرگان حاصل شد. ضمن اینکه تمامی بارهای عاملی سوالات هریک از سازه‌ها از لحاظ آماری معنادار ($P < ۰,۰۰۱$) و مقادیر آن‌ها بیش از ۰,۵ بود، لذا روایی همگرا نیز مورد تایید قرار می‌گیرد (جدول ۲). هم‌چنین برای بررسی روایی واگرای مدل اندازه‌گیری، معیار فورنل و لاکر مورد استفاده قرار گرفته است. روایی واگرا زمانی قابل قبول است که مقدار AVE برای هر سازه، بیشتر از واریانس اشتراکی میان آن سازه و سازه‌های دیگر در مدل باشد (*Fornell & Larcker, 1981*). جدول ۳، ماتریس ضرایب همبستگی میان سازه‌ها و ریشه دوم مقادیر AVE مربوط به هر سازه را نشان می‌دهد. قطر اصلی این ماتریس نشان‌دهنده ریشه دوم میانگین واریانس استخراج‌شده (AVE) را نشان می‌دهد که بر اساس نتایج حاصله از آن و همبستگی‌ها می‌توان به روایی واگرای مدل در سطح سازه بر مبنای معیار فورنل و لاکر پی

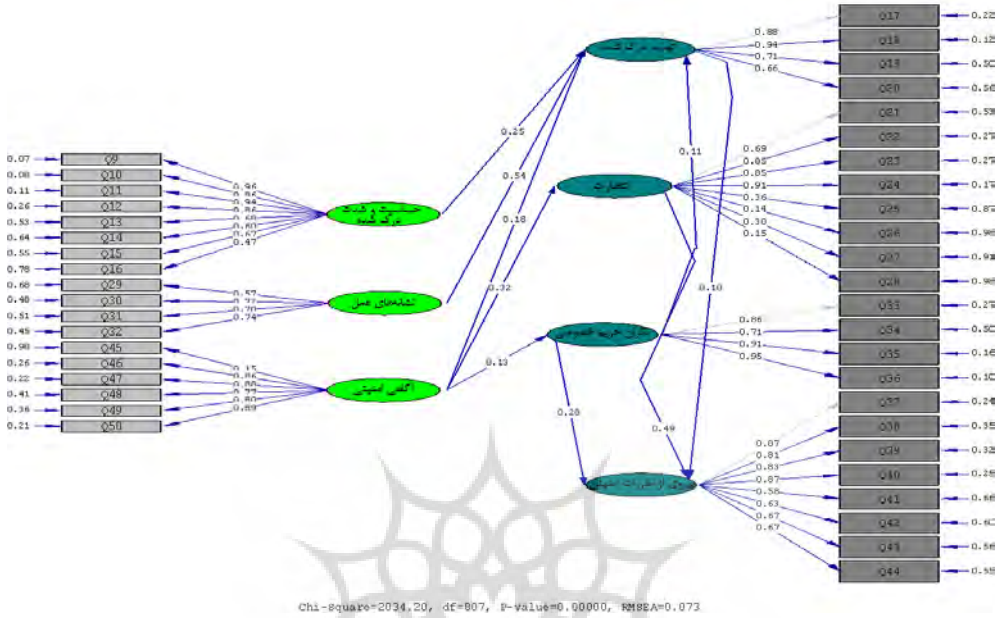
برد؛ زیرا همبستگی تمامی سازه‌ها از جذر شاخص AVE کمتر است. تمامی ضرایب در سطح خطای کمتر از ۰/۰۵ معنادار هستند.

جدول ۳: ضرایب همبستگی و شاخص روایی واگرا

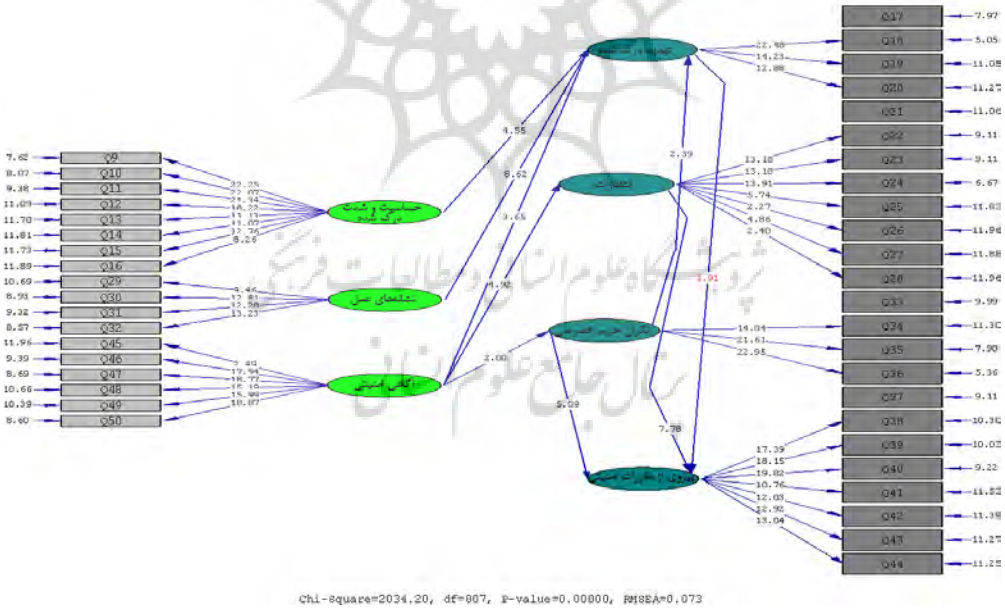
	۱	۲	۳	۴	۵	۶	۷
شدت و حساسیت درک شده	۰/۷۹۴						
تهدید درک شده	۰/۵۲۷	۰/۸۰۵					
انتظارات	۰/۳۵۴	۰/۵۳۳	۰/۷۱۹				
نشانه‌های عمل	۰/۴۰۶	۰/۵۸۶	۰/۶۸۶	۰/۷۳۲			
نگران حریم خصوصی	۰/۳۵۷	۰/۵۲۰	۰/۶۳۰	۰/۶۴۷	۰/۸۶۱		
پیروی از مقررات امنیتی	۰/۲۵۱	۰/۴۲۲	۰/۶۴۷	۰/۵۲۶	۰/۴۷۲	۰/۷۴۸	
آگاهی امنیتی	۰/۰۴۹	۰/۲۰۵	۰/۲۷۵	۰/۰۸۱	۰/۰۸۲	۰/۳۳۱	۰/۸۱۲

یافته‌های پژوهش

پس از جمع‌آوری و تحلیل داده‌ها، مدل‌سازی معادلات ساختاری اجرا و نتایج این مدل‌سازی در شکل‌های ۲ و ۳ قابل مشاهده است. این شکل‌ها به ترتیب مدل‌سازی معادلات ساختاری مدل مفهومی تحقیق از لحاظ تخمین استاندارد و معناداری ضرایب را به تصویر می‌کشند. خلاصه این نتایج در جدول ۴ ارائه شده است.



شکل ۲: مدل‌سازی معادلات ساختاری مدل مفهومی تحقیق (تخمین استاندارد)



شکل ۳: مدل‌سازی معادلات ساختاری مدل مفهومی تحقیق (معناداری ضرایب)

جدول ۴: ضرایب مسیر و آماره‌ی t

فرضیه	ضریب مسیر (β)	آماره t	نتیجه فرضیه
فرضیه ۱	۰/۳۲	۴/۹۲	تائید
فرضیه ۲	۰/۱۳	۲/۰۰	تائید
فرضیه ۳	۰/۱۸	۳/۶۵	تائید
فرضیه ۴	۰/۲۵	۴/۵۵	تائید
فرضیه ۵	۰/۴۹	۷/۷۸	تائید
فرضیه ۶	۰/۲۸	۵/۰۹	تائید
فرضیه ۷	۰/۱۱	۲/۳۹	تائید
فرضیه ۸	۰/۵۴	۸/۶۲	تائید
فرضیه ۹	۰/۱۰	۱/۹۱	رد

با توجه به این نتایج (جدول ۴) می‌توان گفت که فرضیه‌های پژوهش حاضر از لحاظ آماری در سطح $p < ۰۱$ معنادار بوده و به جز فرضیه ۹ (تاثیر تهدید درک‌شده بر پیروی از مقررات امنیتی)، سایر فرضیه‌های پژوهش مورد تایید قرار می‌گیرند.

در ادامه برازش مدل پژوهش مورد ارزیابی قرار گرفت. هدف از برازش مدل این است که مشخص شود آیا روابط تئوریکی که بین متغیرها در مرحله تدوین چارچوب نظری، مد نظر محققین بوده‌اند، به وسیله داده‌های حاصله از پژوهش، مورد تایید قرار گرفته‌اند یا خیر؛ به عبارت دیگر، میزان انطباق مدل با داده‌های تجربی، مشخص شود. مقادیر به‌دست‌آمده از مجموعه شاخص‌های برازندگی که در جدول ۵ آمده است، نشان می‌دهند که مدل پژوهش، از برازش خوب و مناسبی برخوردار است و نتایج شاخص‌های برازش حاکی از برازش مدل مفهومی پژوهش هستند (X^2/df = ۲,۵۲ < ۵ و RMSEA = ۰,۰۷۳ < ۰,۰۸). لذا نیازی به به انجام تعدیل جهت کفایت برازش مدل نیست.

جدول ۵: شاخص‌های برازش مدل مفهومی

نام شاخص	X^2/df	NNFI	IFI	CFI	SRMR	RMSEA
مقدار بدست آمده	۲,۵۲ (۲۰۳۴,۲۰/۸۰۷)	۰,۹۱	۰,۹۴	۰,۹۳	۰,۰۲۳	۰,۰۷۳

بحث و نتیجه‌گیری

با توجه به نتایجی که از آزمون فرضیه‌های پژوهش به دست آمد، مشخص شد که آگاهی امنیتی بر انتظارات (مزایای درک‌شده - موانع درک‌شده)، نگرانی حریم خصوصی و تهدید درک‌شده اثر مثبتی دارد و در واقع با افزایش آگاهی امنیتی منجر به افزایش انتظارات، بهبود نگرانی در مورد حریم خصوصی و افزایش تهدید درک‌شده می‌شود. بنابراین فرضیه‌های اول، دوم و سوم پژوهش مورد تایید قرار گرفتند. در این خصوص می‌توان گفت که هر چه افراد درگیر دورکاری، اطلاعات و آگاهی بیشتری نسبت به مسائل امنیتی مطرح در این حوزه داشته باشند، از تهدیدات موجود مطلع می‌شوند و بیشتر نگران حریم خصوصی خود خواهند شد و در نتیجه انتظارات بیشتری نیز خواهند داشت. این نتایج با نتایج مطالعات انجام‌گرفته توسط الابری و همکاران (۲۰۰۹)، دینو و هارت (۲۰۰۵) و دارسی و همکاران (۲۰۰۹) انطباق دارد.

علاوه بر این، نتایج پژوهش نشان داد که شدت و حساسیت درک‌شده توسط کاربران، اثر مثبتی بر تهدید درک‌شده از سوی آن‌ها دارد و این موضوع منتهی به تایید فرضیه چهارم پژوهش می‌شود. اگرچه تهدید خود یک عامل خارجی محسوب می‌شود، اما درک کاربران از حساسیت و شدت رخدادهای امنیتی باعث افزایش درک آن‌ها از تهدیدات بالقوه می‌شود. این نتایج منطبق بر نتایج مطالعه انجام‌گرفته توسط ادواردز (*Edwards, 2015*) است.

هم‌چنین نتایج حاصل از پژوهش نشان دادند که انتظارات و نگرانی حریم خصوصی، اثر مثبت و معناداری بر پیروی از مقررات امنیتی دارند و بنابراین، فرضیه‌های پنجم و ششم پژوهش نیز مورد تایید قرار گرفتند. هر چه کاربران مزایای امنیتی بیشتری را درک کنند، انتظارات آن‌ها در این حوزه بالاتر رفته و در نتیجه، پیروی آن‌ها از مقررات امنیتی نیز افزایش خواهد یافت. هم‌چنین افزایش نگرانی در مورد حریم خصوصی اطلاعات کاربران، باعث تحریک آن‌ها در جهت رعایت سیاست‌ها و مقررات امنیتی می‌شود. این نتایج کاملا با نتایج حاصل‌شده در مطالعات هومیدی و همکاران (۲۰۱۴) و چو (۲۰۱۰) همخوانی دارد.

در بخش دیگری از نتایج پژوهش مشخص شد که نگرانی حریم خصوصی و نشانه‌های عمل بر تهدید درک‌شده، تاثیر مثبت و معناداری دارند، لذا این موضوع دلالت بر تایید فرضیه‌های هفتم و هشتم پژوهش حاضر دارد. افزایش نگرانی کاربران نسبت به حریم

خصوصی خود باعث افزایش درک آن‌ها نسبت به تهدیدات امنیتی موجود می‌شود و رعایت برخی مسائل امنیتی در عمل نیز نشانه‌ای از درک بیشتر کاربران نسبت به تهدیدات امنیتی است. این نتایج کاملا منطبق بر مطالعات صورت‌گرفته توسط هایدن (۲۰۰۹)، جانز و بکر (۱۹۸۴)، دینو و هارت (۲۰۰۵)، وان اسلایک و همکاران (۲۰۰۶)، انگست و اگروال (۲۰۰۹)، دینو و هارت (۲۰۰۵) و چو (۲۰۱۰) است.

اما نتایج حاصل از تحقیق دلالت بر این موضوع داشتند که تهدید درک‌شده پیرامون مسائل امنیتی، اثر معناداری بر پیروی از مقررات امنیتی ندارد. این موضوع کمی دور از انتظار بود و باعث رد فرضیه نهم پژوهش شد. لیانگ و ژو (۲۰۱۰) دریافتند که تهدید درک‌شده بر انگیزه اجتنابی تاثیر دارد، اما تاثیر آن بر رفتار اجتنابی را آزمایش نکردند. اگرچه ادواردز (۲۰۱۵) نیز در مطالعه خود به این نتیجه رسید که تهدید امنیتی درک‌شده بر رفتار امنیتی و پیروی از مقررات امنیتی تاثیر معناداری ندارد.

به طور خلاصه، یافته‌های این پژوهش نشان می‌دهند که اکثریت کاربران دورکار تا حدی از مسائل امنیتی (به ویژه در حوزه مهندسی اجتماعی) آگاهی دارند. اگرچه این موضوع مستقیما بر پیروی از مقررات و سیاست‌های امنیتی سازمان‌ها اثرگذار نیست، اما بر انتظارات، نگرانی حریم خصوصی و تهدید درک‌شده تاثیرگذار است. هم‌چنین انتظارات و نگرانی حریم خصوصی، خود بر پیروی از مقررات امنیتی در سازمان‌ها تاثیر مثبت و معناداری دارند، اما تهدید درک‌شده فاقد اثر معناداری بر پیروی از این مقررات است.

بر اساس نتایج فوق می‌توان به مدیران سازمان‌ها (خصوصا مدیران امنیت و فناوری اطلاعات) توصیه کرد که با برگزاری دوره‌های آگاهی‌رسانی و آموزش در حوزه امنیت اطلاعات، آگاهی پرسنل خود را نسبت به مسائل امنیتی مطرح در مورد دورکاری بالاتر ببرند تا در صورت بروز حوادث و وقایعی (مانند شیوع بیماری همه‌گیر کووید-۱۹) که بالاجبار باعث دورکاری آن‌ها می‌شود، مقررات امنیتی سازمان را در فعالیت‌های سازمانی خود رعایت کنند تا این اتفاق باعث به خطر افتادن داده‌ها و اطلاعات سازمان نشود.

هم‌چنین کاربران دورکار که مجبور هستند برای ارسال اطلاعات خود به سازمان از بستر اینترنت استفاده کنند، باید آگاهی و توجه خود را در هنگام استفاده از این فناوری، نسبت به تهدیدات وارد بر آن بالاتر ببرند. اگرچه این موضوع خود مستقیما باعث رعایت مقررات

امنیتی نمی‌شود، اما با افزایش این آگاهی می‌توان پی به مسائلی در مورد حریم خصوصی و مزایا و موانع امنیتی برد و سپس با برخورداری از درکی بالاتر پیرامون این مسائل، مقررات امنیتی سازمان را با دقت بیشتری رعایت کرد.

این پژوهش با محدودیت‌هایی نیز مواجه بود. سایر محققان در آینده می‌توانند با غلبه بر چنین محدودیت‌هایی، ارزش بیشتری را در مطالعات حوزه امنیت اطلاعات و دورکاری بیافرینند. هم‌چنین این پژوهش صرفا با خوداظهاری افراد شرکت‌کننده صورت گرفته است. از این رو، در راستای تکمیل و توسعه پژوهش حاضر پیشنهادهای ذیل برای پژوهش‌های آتی ارائه می‌شود:

۱) در پژوهش آتی می‌توان متغیرهایی مانند فرهنگ امنیتی سازمان یا شخص را نیز به مدل افزود تا اثر آن بر پیروی پرسنل سازمان از مقررات امنیتی نیز مورد سنجش قرار گیرد.

۲) پژوهش‌های آینده به دنبال مشاهده و ثبت رفتارهای امنیتی افراد دورکار (به صورت نامحسوس) در عمل باشند تا بیان احتمالی خلاف واقعیت از سوی افراد شرکت‌کننده در پژوهش، نتایج پژوهش را تحت تاثیر قرار ندهد.

۳) در نهایت می‌توان اثرات این همه‌گیری (و به دنبال آن دورکاری) را از سایر جنبه‌ها مانند تاثیر آن بر عملکرد سازمانی یا رضایت شغلی کارکنان، نیز بررسی کرد.

References

1-Al Abri, D., McGill, T., & Dixon, M. (2009). Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: An Oman perspective. Journal of Information Privacy & Security, 5(2), 3-26.

2-Angst, C. M. & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS Quarterly, 33(2), 339-370.

3-Anti-Phishing Working Group. (2011). Phishing activity trends report 1st half / 2011. Retrieved December 15, 2015, from http://www.antiphishing.org/reports /apwg_trends_report_h1_2011.pdf

4-Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes, 50, 179-211.

5-Bagozzi, R. P. & Yi, Y. (1988). On the evaluation of structural equation models. Journal of the Academy of Marketing Science, 16(1), 74-94.

7-Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010, January). Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation. In 2010 43rd Hawaii International Conference on System Sciences (pp. 1-7). IEEE.

8-Cho, H. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. Journal of Information Privacy & Security, 6(1), 3-27.

9-Cho, H., Rivera, M., & Lim, S. (2009). A multinational study on online privacy: Global concerns and local responses. New Media & Society, 11(3), 409-431.

10-Claar, C. L. (2011). The adoption of computer security: An analysis of home personal computer user behavior using the health belief model. Utah State University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 3449480.

11-Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd ed.), Lawrence Erlbaum Associates.

12-Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers & Security, 26, 63-72

13-Chakraborty, I., & Maity, P. (2020). COVID-19 outbreak: Migration, effects on society, global environment and prevention. Science of the Total Environment, 138882.

14-D'Aryy J Hvvvv A & Gll lett D (0009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98.

15-Dinev, T. & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7-29.
16-Edwards, K. (2015). Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing.
17-Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Boston, MA: Addison-Wesley.
18-Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.
19-Ghauri, P., Grønhaug, K., & Strange, R. (2020). Research methods in business studies. Cambridge University Press.
20-Gay, L. R., Mills, G. E., & Airasian, P. (2009). Educational research competencies for Analysis and Applications (9th ed.), pp. 129-131, 155-157. Upper Saddle River, NJ: Pearson Education, Inc.
21-Glanz, K., Rimer, B. K., & Viswanath, K. (2008). Health Behavior and Health Education: Theory, Research, and Practice (4th ed.). John Wiley and Sons.
22-Grant, G. J. (2010). Ascertaining the relationship between security awareness and the security behavior of individuals. Nova Southeastern University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 3423144.
23-Hayden, J. (2009). Introduction to health behavior theory. Burlington, MA: Jones & Bartlett Learning.
24-Hochbaum, G. M. (1958). Public participation in medical screening programs: A sociopsychological study. Public Health Service Publication No. 572. Washington, D.C., 1-23.
25-Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014). Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model. 2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), 30-35.
26-Jafari, M. S., Hamidizadeh, A., & Montazeri Najafabadi, R. (2016). Investigating the effective factors on employees' compliance with information systems security policies in the organization. Scientific Journal of Information Management, 2(2), 102-131. (in persian)
27-Janz, N. K. & Becker, M. H. (1984). The Health Belief Model: A decade later. Health Education Quarterly, 11(1), 1-47.

28-Koloseni, D. N., Lee, C. Y., & Gan, M. (2019). Understanding Information Security Behaviours of Tanzanian Government Employees: A Health Belief Model Perspective. International Journal of Technology and Human Interaction (IJTHI), IGI Global, vol. 15(1), 15-32, January.

29-Kritzinger, E. & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 29, 840-847.

30-Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25, 289-296.

31-Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413.

32-Mirnezami, S., & Rajabi, S. (2020). Estimating the Impacts of COVID-19 on Iran Economy: Modelling 7 Scenarios. Science and Technology Policy, 10(2).

33-Nardi, P. M. (2003). Doing Survey Research: A guide to quantitative methods. Boston, MA: Pearson Education, Inc.

34-Nasri, A., Bagheri, A., & Boushehri, A. (2020). Assessing the Role of Governmental Support in Strategy Formation of Knowledge-based Enterprises Facing Coronavirus Pandemic Consequences. Science and Technology Policy, 10(2).

35-Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46, 815-825.

36-Payande, I., Majdizade, Z., Mirzapour, H. (2020). In Search of an Alternative to "Strict Lockdown"; Data-driven Policies in the Face of COVID-19 Pandemic. Science and Technology Policy Letters, 10(2), 59-73.

37-Rea, L. M. & Parker, R. A. (2005). Designing & conducting survey research: A comprehensive Guide (3rd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

38-Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information eeuurity:. It iff leeeee ss rr '' iff rr mtt io eerrr ity rr att iee hhhvvirr . Computers & Security, 28, 816-826.

39-Ross, T. P., Ross, L. T., Rahman, A., & Cataldo, S. (2010). The bicycle helmet attitudes scale: using the health belief model to predict helmet use among undergraduates. Journal of American College Health, 59(1), 29-36.

40-Rovai, A. P., Baker, J. D., & Ponton, M. K. (2014). Social Science Research Design and Statistics: A Practitioner's Guide to Research Methods and IBM SPSS Analysis (2nd ed.), p. 419. Watertree Press LLC. Kindle Edition.

41-Straub, D. W. (1989). Validating instruments in MIS research. MIS Quarterly, 13(2), 147-169.

42-Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for is positivist research. Communications of the Association for Information Systems, 13, 380-427.
43-Styles, M. & Tryfonas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. Information Management & Computer Security, 17(1), 44-52.
44-Trochim, W. M. K. & Donnelly, J. P. (2008). The research methods knowledge base (3rd ed.), pp. 56-65. Mason, OH: Atomic Dog.
45-Van Slyke, C., Shin, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(6), 415-431, 433-443.
46-Weiers, R. M. (2002). Introduction to Business Statistics (4th ed.). Belmont, CA: Duxbury, Thomson Learning.