Evaluating the Behavior of Users of Mobile Electronic Devices with the Emphasis on Protection Motivation Theory of Data Breach: a Case Study of Graduate Students

Faramarz Soheili
PhD in Knowledge and Information Science; Associate Professor; Department of Knowledge and Information Science; Payame Noor University; Tehran, Iran Email: fsohieli@gmail.com

Reza Rostaei
MSc. Student; Department of Knowledge and Information Science; Payame Noor University; Tehran, Iran;
Email: rezaroustaei97@gmail.com

Ali Akbar Khasseh
PhD in Knowledge and Information Science; Associate Professor; Department of Knowledge and Information Science; Payame Noor University; Tehran, Iran Email: khasseh@gmail.com

Mehri Shahbazi*
PhD in Knowledge and Information Science; Assistant Professor; Department of Knowledge and Information Science; Payame Noor University; Tehran, Iran Email: meh512000@yahoo.com

Iranian Journal of Information Processing and Management

Received: 20, Aug. 2020 **Accepted: 07, Feb. 2021**

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 36 | No. 4 | pp. 1137-1158
Summer 2021

Abstract: This study tries to evaluate the experimental behavior of graduate students of Ilam University when using mobile electronic devices (mobile phones, tablets and laptops) based on the protection motivation theory of data breach. This research is of applied-survey type. The statistical population of research includes graduate students of Ilam University. Data collection tool was based on the questionnaires introduced by Boss et al., Woon et al., Claar and Johnson, Johnson and Warkentin, and Posey et al. For data analysis, structural equation modeling was used to fit the model and test the hypotheses of research in AMOS software using partial least squares method. Results indicated that there is a positive relationship between the perceived threat sensitivity, response effectiveness, self-efficacy and the possibility of using the security of mobile electronic devices with the protection motivation. In

* Corresponding Author

addition, the findings showed that there is not a meaningful relationship between the perceived threat intensity and the motivation of protecting the mobile electronic devices. There is a negative (indirect) relationship between the perceived response cost and the protection motivation. Generally, this study emphasized that the confrontational assessment process is a more important factor than the threat assessment process in increasing users' protection motivation.

Keywords: Mobile Rlectronic Devices, Protection Motivation Theory, Data Breach

ارزیابی رفتار کاربران ابزارهای الکترونیکی سیار با تأکید بر نظریهٔ انگیزهٔ محافظت از نقض داده‌ها

مطالعهٔ موردی: ارزیابی رفتار دانشجویان تحصیلات تکمیلی

فرامرز سهیلی
دکتری علم اطلاعات و دانش‌شناسی؛ دانشیار؛ گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور؛ تهران، ایران fsohieli@gmail.com

رضا روستایی
کارشناسی ارشد علم اطلاعات و دانش‌شناسی؛ دانشگاه پیام نور؛ تهران، ایران؛ rezaroustaei97@gmail.com

علی‌اکبر خاصه
دکتری علم اطلاعات و دانش‌شناسی؛ دانشیار؛ گروه علم اطلاعات و دانش‌شناسی؛ دانشگاه پیام نور؛ تهران، ایران khasseh@gmail.com

مهری شهبازی
دکتری علم اطلاعات و دانش‌شناسی؛ استادیار؛ گروه علم اطلاعات و دانش‌شناسی؛ دانشگاه پیام نور؛ تهران، ایران؛
پدیدآور رابط meh512000@yahoo.com

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۳۹۹/۰۵/۳۰ | پذیرش: ۱۳۹۹/۱۱/۱۹ | مقاله برای اصلاح به مدت ۵۰ روز نزد پدیدآوران بوده است.

چکیده: ارزیابی رفتار تجربی کاربران هنگام استفاده از ابزارهای الکترونیکی سیار (موبایل، لپ‌تاپ، تبلت) بر اساس نظریهٔ انگیزهٔ محافظت از نقض داده‌ها هدف اصلی پژوهش حاضر است. این پژوهش از نوع کاربردی- پیمایشی است و دانشجویان تحصیلات تکمیلی دانشگاه ایلام در سال ۱۳۹۸ جامعهٔ آماری پژوهش را تشکیل می‌دهند. ابزار گردآوری داده‌ها بر اساس پرسشنامه‌های استاندارد «باس» و همکاران، «وون، جک‌وود و لو»، «کلار و جانسون»، «جانسون و وارکنتین»، و «پوزی، ربرتس و لوری» ساخته شد و در تجزیه و تحلیل داده‌ها جهت برازش مدل و آزمون فرضیه‌های پژوهش از مدل‌یابی معادلات ساختاری با به‌کارگیری روش حداقل مربعات جزئی در نرم‌افزار «آموس» استفاده شد. یافته‌های پژوهش نشان داد که

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۶ | شمارهٔ ٤ | ص‌ص ۱۱۳۷-۱۱۵۸
تابستان ۱۴۰۰

بین حساسیت تهدید درک‌شده، اثربخشی پاسخ، خودکارآمدی و احتمال استفاده از امنیت ابزارهای الکترونیکی سیار با انگیزهٔ محافظت رابطهٔ مثبت، و بین هزینهٔ پاسخگویی درک‌شده و انگیزهٔ محافظت رابطهٔ منفی وجود دارد. اما بین شدت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود ندارد. نتایج پژوهش همچنین نشان داد که ارزیابی کاربران از حساسیت‌های خود در برابر تهدیدات و میزان اعتماد به توانایی‌های خود در جهت استفادهٔ مناسب از امکانات امنیتی ابزارهای الکترونیکی سیار و خودکارآمدی دستگاه‌ها و اثربخشی پاسخ تعیین‌کنندهٔ میزان انگیزهٔ آنان در انجام اقدامات محافظتی است و افزایش یا کاهش انگیزهٔ محافظت، تعیین‌کنندهٔ میزان استفاده از امنیت ابزارهای الکترونیکی سیار است. در کل، این پژوهش بر این نکته تأکید دارد که فرایند ارزیابی مقابله‌ای نسبت به فرایند ارزیابی تهدید عامل مهم‌تری در افزایش انگیزهٔ محافظت کاربران است.

کلیدواژه‌ها: ابزارهای الکترونیک سیار، نظریهٔ انگیزهٔ حفاظت، نقض

۱. مقدمه

رشد و توسعهٔ چشمگیر و جهانیِ فناوری‌های اطلاعات و ارتباطات در سال‌های اخیر، کاربردهای جدید و فراوان فناوری‌های همراه و خدمات آن را به‌دنبال داشته و به‌تبع این افزایش کاربرد، میزان استفاده از این فناوری‌ها نیز افزایش یافته است. امروزه، افراد، بسیاری از اطلاعات خود را در ابزارهای الکترونیکی سیار مثل رایانه‌های همراه، گوشی‌های هوشمند و تبلت‌ها ذخیره می‌کنند. اگرچه رشد استفاده از ابزارهای الکترونیکی سیار را می‌توان ناشی از راحتی آن‌ها دانست، اما کاربران این دستگاه‌ها با معضلی به نام سرقت داده‌ها و نقض داده‌ها روبه‌رو هستند (Giwah et al. 2020). به بیان دیگر، هر کدام از این ابزارها با درجه‌ای از تهدید و نفوذ غیر مجاز همراه هستند. افزایش استفاده از ابزارهای الکترونیکی سیار رفتار اطلاعاتی کاربران را نیز تغییر داده است و این‌گونه به نظر می‌رسد که اطلاع‌یابی کاربران در این نوع ابزارها با سرعت بیشتر و در برخی موارد دقت و اطمینان کمتر همراه است. افزون بر این، در گذشته، امنیت افراد و اطلاعات متناسب با محیط، از طریق حضور فیزیکی و نظارت تأمین می‌شد، اما در سال‌های اخیر که در جهان شاهد به‌کارگیری تجهیزات الکترونیکی و روش‌های مجازی برای برقراری ارتباطات و تبادل اطلاعات هستیم، بحث امنیت به‌ویژه در حوزهٔ اطلاعات به میزان قابل توجهی رشد و تکامل یافته است. متناسب با گسترش فناوری، روش‌های مختلف حمله به ابزارهای فناورانهٔ ارتباطی و اطلاعاتی نیز توسعه یافته و امنیت را چه از نظر ارتباطی یا اطلاعاتی در معرض خطر قرار داده است. از این رو، بحث امنیت اطلاعات و محافظت از آن‌ها نقطهٔ

تمرکز متفاوتی شده و چالش بزرگی را برای کاربران ایجاد کرده است.

«کریمی و پیکری» معتقدند که بیشترین دلایل نقض امنیت اطلاعات به عامل‌های مربوط به افراد برمی‌گردد (۱۳۹۷). رویکرد انسانی بر خلاف رویکرد فنی که استفاده از ابزارهایی مانند آنتی‌ویروس یا گذرواژهٔ قوی و مسائلی از این قبیل را موجب حفظ امنیت اطلاعات در ابزار می‌داند، به این مسئله گرایش دارد که اتخاذ عوامل فنی به رفتار کاربر بستگی دارد. از این رو، رفتار فرد به اندازهٔ رویکرد فنی از اهمیت برخوردار است. بنا بر رویکرد انسانی و با وجود اعمال کنترل‌های فنی، اگر یک شخص بعد از وارد شدن به ابزار مورد استفاده، آن را خاموش نکند یا آن را در مکانی جا بگذارد، یا گذرواژهٔ مناسبی برای آن انتخاب نکند و رفتاری از این قبیل داشته باشد، دیگر کنترل فنی نمی‌تواند امنیت اطلاعات را تأمین کند و برای امنیت اطلاعات باید به مسائل انسانی توجه شود.

در دهه‌های گذشته، مدل‌ها و چارچوب‌های نظری زیادی برای بررسی رفتارهای انسان و پذیرش فناوری مورد استفاده قرار گرفته که از آن جمله می‌توان به نظریهٔ «انگیزهٔ محافظت»[1] (Rogers (1975, 1983 اشاره کرد. این نظریه را وی نخستین‌بار در سال ۱۹۷۵ ارائه کرد و مدل باورهای سلامت را با تأکید بر فرایندهای شناختی مرتبط با تغییرات رفتاری و نگرش مورد استفاده قرار داد تا درک مفهومی واضحی از نظریهٔ «توسل به ترس»[2] را ارائه دهد. این نظریه شامل دو مرحلهٔ مهم ارزیابی تهدید (حساسیت به تهدید درک‌شده، شدت تهدید درک‌شده و پاداش‌های درک‌شده) و ارزیابی کنار آمدن (خودکارآمدی درک‌شده، اثربخشی درک‌شده و هزینه‌های درک‌شده) و سازهٔ بینابینی ترس است (Rogers 1975). «ایفیندو» معتقد است که فرایند ارزیابی تهدید به این دلیل ایجاد شد که فرد قبل از ارزیابی رفتارهای مقابله، نیاز به تشخیصِ تهدید دارد و در حقیقت، رفتارهای ناسازگارانه و عوامل مؤثر بر احتمال درگیرشدن در رفتارهایی را که به‌طور بالقوه ناسالم هستند، بررسی می‌کند و شامل پاداش‌های درونی و بیرونی همراه با رفتارهای ناسالم و درک تهدید (مجموع حساسیت و شدت تهدید درک‌شده) است (Ifinedo 2012).

ارزیابی تهدید شامل شدت تهدید درک‌شده[3]، حساسیت به تهدید درک‌شده[4] و پاداش‌هاست. شدت تهدید درک‌شده باور فرد از میزان تهدید است، در حالی که

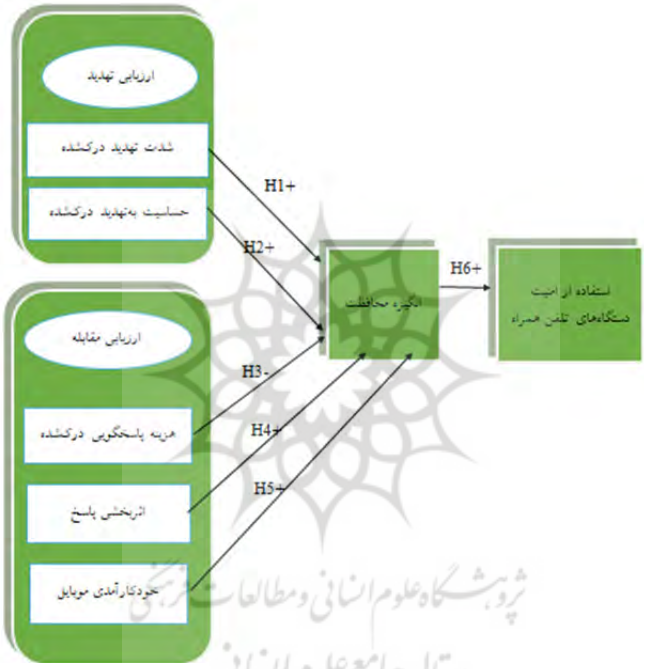
1. theory of protection motivation
2. fear appeal
3. perceived threat severity
4. perceived threat susceptibility

حساسیت به تهدید درک‌شده باور فرد از احتمال تجربهٔ تهدیدی خاص است. پاداش‌ها شامل مزایای درونی و بیرونی کسب‌شده توسط فرد برای عدم انجام واکنش توصیف‌شده است. در زمینهٔ امنیت اطلاعات، «ونس، سیپونن و پانیلا» به پاداش‌ها به‌عنوان صرفه‌جویی در زمان به‌وسیلهٔ عدم رعایت سیاست امنیت اطلاعات اشاره می‌کنند (Vance, Siponen & Pahnila 2012).

فرایند ارزیابی مقابله که توانایی مقابله و دفع خطر تهدیدشده را ارزیابی می‌کند، هنگامی ایجاد شد که فرد به‌دنبال ابزارهای محافظت در مقابل میزان آسیب ایجادشده از سوی تهدید بود. این فرایند شامل ملاحظهٔ تأثیر و هزینهٔ مقابله است. توانایی مقابله و دفع خطر تهدیدشده با ارزیابی مقابله مشخص می‌شود. افزایش ارزیابی مقابله باعث افزایش انگیزش محافظت و در نتیجه، افزایش احتمال انجام رفتار می‌شود و شامل خودکارآمدی درک‌شده[1]، اثربخشی درک‌شده[2] و هزینه‌های پاسخ درک‌شده[3] است. اثربخشی پاسخ عبارت است از انتظار شخص از این‌که پاسخ سازگار (محافظت از خود) می‌تواند تهدید را از بین ببرد و انتظار می‌رود که مؤثر بودن رفتار پیشنهادی پیشگیری‌کننده باعث افزایش پاسخ شود (Floyd, Prentice-Dunn & Rogers 2000). خودکارآمدی در حقیقت اعتقاد فرد به این است که او توانایی انجام درست رفتارهای سازگارانه و رفتارهای توصیه‌شده را دارد. در واقع، سطح اطمینان از توانایی فرد برای به‌عهده گرفتن رفتار پیشگیری‌کننده توصیه شده و نیز توانایی غلبه بر هزینه‌هاست (Floyd, Prentice-Dunn & Rogers 2000; Crismaru 2006). انتظار می‌رود که درک خودکارآمدی بالا باعث پاسخ‌گویی مثبت بیشتر در فرد شود. هزینه‌های پاسخ شامل هزینه‌های مالی و غیر مالی مثل زمان، تلاش و کوشش، ناراحتی، دردسر، رنج و مانند آن است که به‌عنوان موانع ایجاد رفتار پیشگیری‌کننده است (Crismaru 2006). افزایش هزینه در به‌کار گرفتن رفتارهای محافظت‌کننده باعث کاهش انگیزش انجام رفتارهاست. ارزیابی مقابله از مجموع اثربخشی پاسخ و خودکارآمدی درک‌شده منهای هزینه‌های پاسخ به‌دست می‌آید. بدین‌ترتیب، افزایش اثربخشی پاسخ و خودکارآمدی و کاهش هزینه‌های پاسخ باعث افزایش ارزیابی مقابله می‌شود. بازده دو فرایند میانجی شناختی باعث شکل‌گیری انگیزش محافظت فراخوانده می‌شود. شدت درک‌شدهٔ تهدید و آسیب‌پذیری درک‌شدهٔ تهدید باید بر پاداش‌های پاسخ ناسازگار

1. perceived self-efficacy 2. perceived efficiency 3. perceived costs

(عدم محافظت از خود) غلبه کند و خودکارآمدی درک‌شده و اثربخشی پاسخ درک‌شده باید بر هزینه‌های پاسخ سازگار (محافظت از خود) نیز غلبه داشته باشد. انگیزش محافظت به‌عنوان یک متغیر واسطه‌ای بین مراحل ارزیابی تهدید، ارزیابی مقابله و رفتار پیشگیری‌کننده (رفتار حفاظت‌کننده) است (Floyd, Prentice-Dunn & Rogers 2000). «گیوا» این روابط را به‌صورت مدلی در پژوهش خود ارائه کرد (Giwah 2019). این مدل اساس مدل مفهومی پژوهش حاضر را به خود اختصاص داد (شکل ۱).



شکل ۱. مدل مفهومی پژوهش (اقتباس از پژوهش Giwah 2019)

بررسی‌ها نشان می‌دهد که نظریهٔ انگیزهٔ محافظت، نخست برای شناخت ارزیابی ترس ارائه شده و بعدها به‌منظور شناخت فرایند شناختی تعدیل‌کننده (واسطه‌گر) تغییر رفتاری، توسعه یافته است (Floyd, Prentice-Dunn & Rogers 2000). این نظریه مورد توجه بسیاری از پژوهش‌ها بوده و به‌طور گسترده‌ای در پژوهش‌های امنیت اطلاعات به‌منظور شناخت فرایند ارزیابی تهدید و ارزیابی مقابله در رفتارهای امنیت اطلاعاتی (Anderson and Agarwal 2010; 2010; Johnston and Warkentin Giwah 2019;) و تطبیق سیاست‌های امنیتی (Herath and Rao 2009; Ifindeo 2012; Vance, Siponen & Pahnila 2012) مورد استفاده قرار

گرفته است. بیشتر مطالعات صورت‌گرفته در زمینهٔ حفاظت اطلاعات به بررسی امنیت اطلاعات در سیستم‌های اطلاعاتی و سازمان‌ها پرداخته (محمودزاده و رادرجبی ۱۳۸۵؛ پیکری و بنازاده ۱۳۹۷؛ کریمی و پیکری ۱۳۹۷؛ Herath and Rao 2009; Kim et al. 2014; Johnston and Warkentin 2010; Vance, Siponen & Pahnila 2012; Posey, Roberts & Lowry 2015; Park, Kim & Park 2017; Veiga & Martins 2017) و تعداد محدودی از این پژوهش‌ها به بررسی امنیت ابزارهای الکترونیکی سیار و اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی و غیره پرداخته‌اند (خارا و صارمیان ۱۳۹۴؛ حسینی دوزین ۱۳۹۵؛ حسینی سنو و مظاهری ۱۳۹۷؛ Dang-Pham & Pittayachawan 2015; Giwah 2019; Mousavi et al. 2020). منظور از استفاده از امنیت ابزارهای الکترونیک سیار، استفادهٔ واقعی از ویژگی‌ها و اجزای امنیتی این ابزارهاست. این ویژگی‌های امنیتی شامل ضد ویروس[1]، ضد بدافزار[2]، تهیهٔ نسخهٔ پشتیبان[3]، دیوار آتش (فایروال[4])، بررسی و اجرای نرم‌افزارها و به‌روزرسانی‌های سیستم عامل و احراز هویت قوی هستند (Claar and Johnson 2012).

بررسی پژوهش‌های موجود، وجود پیشینه‌ای در زمینهٔ رفتار امنیت اطلاعات کاربران ابزارهای الکترونیکی سیار در ایران را نشان نداد و در خارج از کشور نیز تنها پژوهش یافت‌شده در این مورد پژوهش Giwah (2019) بود که رفتار امنیت اطلاعاتی کاربران دستگاه‌های تلفن همراه را مورد مطالعه قرار داده بود. بنابراین، می‌توان گفت که کاربست این نظریه یک موضوع پژوهشی جدید در حیطهٔ فناوری اطلاعات و ارتباطات به‌طور عام و امنیت اطلاعات در ابزارهای الکترونیکی سیار، مانند موبایل، لپ‌تاپ و تبلت به‌طور خاص است. با توجه به این‌که طبق تعریف، نقض داده‌ها، هنگام دسترسی به اطلاعات شخصی توسط اشخاص غیر مجاز به‌دلیل آسیب‌پذیری‌های امنیتی توسط هکرها، گم‌شدن دستگاه‌ها، اشخاص ثالث غیرمجاز و غیره رخ می‌دهد (Culnan and Williams 2009) و با تأکید بر کاربرد و استفادهٔ زیاد از ابزارهای الکترونیکی سیار و نیز احتمال عدم رعایت مسائل امنیتی از جانب کاربران، پرداختن به این موضوع حائز اهمیت به نظر می‌رسد. از آنجا که نقض امنیت و در معرض دید قرار گرفتن داده‌ها و اطلاعات کاربران در دنیای امروز بیش از پیش روی می‌دهد (Douglas 2019)، کنکاش پیرامون این معضل و چگونگی برخورد کاربران با آن می‌تواند دانسته‌های جدیدی فراروی ما قرار دهد. از

1. anti-virus 2. antimalware 3. backup 4. firewall

این رو، پژوهش حاضر بر آن است که با استفاده از نظریهٔ انگیزهٔ محافظت، به‌طور خاص به ارزیابی رفتار امنیت اطلاعات کاربران در هنگام استفاده از ابزارهای الکترونیکی سیار بپردازد. با توجه به این‌که قشر دانشجو از جملهٔ کاربران حرفه‌ای ابزارهای الکترونیکی سیار به‌ویژه به‌منظور استفاده‌های پژوهشی و آموزشی هستند، در این پژوهش تلاش می‌شود با توجه به مدل مفهومی انگیزهٔ محافظت (شکل ۱) به بررسی رفتار تجربی این دسته از کاربران هنگام استفاده از ابزارهای الکترونیکی سیار (موبایل، لپ‌تاب، تبلت) پرداخته شود. بر این اساس، با توجه به مدل ذکرشده، به تعیین رابطه بین شدت تهدید درک‌شده، حساسیت به تهدید درک‌شده، هزینهٔ پاسخگویی درک‌شده، اثربخشی پاسخ و خودکارآمدی با انگیزهٔ محافظت از ابزارهای الکترونیکی سیار پرداخته و در نهایت، رابطهٔ «انگیزهٔ محافظت کاربران» با «احتمال استفاده از امنیت ابزارهای الکترونیکی سیار» را مورد توجه قرار می‌دهیم. در راستای تحقق این امر، فرضیه‌های زیر در این پژوهش مورد بررسی قرار گرفت:

۱. بین شدت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد؛
۲. بین حساسیت به تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد؛
۳. بین هزینهٔ پاسخگویی درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد؛
۴. بین اثربخشی پاسخ و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد.
۵. بین خودکارآمدی و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد؛
۶. بین انگیزهٔ محافظت و احتمال استفاده از امنیت ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد.

۲. روش پژوهش

پژوهش حاضر از نظر هدف، کاربردی، از نظر میزان کنترل متغیرها، همبستگی و از بعد روش اجرا، پیمایشی است.

جامعهٔ آماری پژوهش حاضر را کلیهٔ دانشجویان تحصیلات تکمیلی دانشگاه ایلام (۱۲۱۶ نفر) در سال ۱۳۹۸-۱۳۹۹ تشکیل دادند که طبق فرمول «کوکران» از میان آن‌ها ۲۹۲ نفر به‌عنوان نمونه به‌صورت تصادفی انتخاب شدند.

برای گردآوری داده‌های مورد نظر پژوهش از پرسشنامه‌ای شامل ۷ سازهٔ اصلی مشخص‌شده در فرضیه‌های این پژوهش استفاده شد. در این پرسشنامه منظور از ارزیابی تهدید نمره‌ای است که فرد از پرسشنامهٔ شدت تهدید درک‌شده و حساسیت به تهدید درک‌شده کسب می‌کند و منظور از ارزیابی مقابله نمره‌ای است که فرد از پرسشنامهٔ هزینهٔ پاسخگویی درک‌شده اثربخشی پاسخ و خودکارآمدی کسب می‌کند. در تهیهٔ ابزار این پژوهش از پرسشنامه‌های استانداردهای ذکرشده در جدول ۱، در مقیاس ۵ درجه‌ای «لیکرت» استفاده شد.

جدول ۱. پرسشنامه‌های استاندارد استفاده‌شده در تهیهٔ پرسشنامهٔ پژوهش

ردیف	برای سنجش مؤلفه	پرسشنامهٔ استاندارد	تعداد گویه
۱	شدت تهدید درک‌شده	Claar & Johnson (2012)	۵
۲	حساسیت به تهدید درک‌شده	Claar & Johnson (2012)	۵
۳	هزینهٔ پاسخ‌گویی درک‌شده	Boss et al. (2015); Woon, Gekwood and L Low (2005)	۸
۴	اثربخشی پاسخ	Boss et al. (2015); Johnston & Warkentin. (2010)	۶
۵	خودکارآمدی	Claar & Johnson (2012)	۴
۶	انگیزهٔ محافظت	Posey, Roberts & Lowry (2015)	۳
۷	امنیت دستگاه	Claar & Johnson (2012)	۸

به‌منظور تجزیه و تحلیل داده‌ها در پژوهش حاضر با استفاده از نرم‌افزار «آموس»[1] شاخص‌های چولگی و کشیدگی و مدل‌یابی معادلات ساختاری با به‌کارگیری روش حداقل مربعات جزئی[2] استفاده شد.

جهت سنجش روایی پرسشنامه از نظرات اساتید متخصص در این زمینه استفاده شد و به‌منظور برآورد پایایی در پژوهش حاضر فرمول آلفای «کرونباخ» به‌کار گرفته شد. به این منظور، پرسشنامهٔ نهایی قبل از شروع پژوهش بین ۴۰ نفر از دانشجویان توزیع و جمع‌آوری

1. Amos
2. partial least squares (PLS)

گردید. آلفای «کرونباخ» پرسشنامه‌ها (جدول ۲) نشان‌دهندهٔ پایایی قابل قبولی است.

جدول ۲. ضریب آلفای «کرونباخ» جهت بررسی پایایی پرسشنامه

ردیف	متغیر	تعداد گویه‌ها	مقدار آلفای کرونباخ
۱	شدت تهدید درک‌شده	۵	۰/۸۱۱
۲	حساسیت به تهدید درک‌شده	۵	۰/۷۷۱
۳	هزینهٔ پاسخگویی درک‌شده	۸	۰/۷۸۶
۴	اثربخشی پاسخ	۶	۰/۷۱۰
۵	خودکارآمدی	۷	۰/۹۱۰
۶	انگیزهٔ محافظت	۳	۰/۸۵۵
۷	استفاده از امنیت دستگاه	۸	۰/۷۹۰

۳. یافته‌های پژوهش

۳-۱. شاخص‌های توصیفی پژوهش

توزیع فراوانی پاسخ‌دهندگان بر حسب متغیرهای جمعیت‌شناختی جنسیت، سطح تحصیلات، سن و میزان استفاده آن‌ها از ابزارهای الکترونیکی سیار (جدول ۳) نشان می‌دهد که بیشترین تعداد پاسخ‌دهندگان از نظر جنسیت زن، از نظر مقطع تحصیلی دانشجوی مقطع کارشناسی ارشد، و از نظر سن بین ۲۶ تا ۳۵ سال بوده و ۳۷ درصد آن‌ها بین ۳ تا ۵ سال است که از ابزارهای الکترونیکی سیار استفاده می‌کردند.

جدول ۳. توزیع فراوانی پاسخ‌دهندگان بر حسب متغیرهای جمعیت‌شناختی

جنسیت	فراوانی	درصد فراوانی	تحصیلات	فراوانی	درصد فراوانی
مرد	۱۲۹	۴۴/۲	کارشناسی‌ارشد	۱۸۵	۶۳/۴
زن	۱۶۳	۵۵/۸	دکتری	۱۰۷	۳۶/۶
کل	۲۹۲	۱۰۰	کل	۲۹۲	۱۰۰
سن	۱۸ - ۲۵	۲۶ - ۳۵	۳۶ - ۴۵	۴۶ - ۵۵	کل
فراوانی	۸۲	۱۲۴	۶۹	۱۷	۲۹۲
درصد فراوانی	۲۸/۱	۴۲/۵	۲۳/۶	۵/۸	۱۰۰

جنسیت	فراوانی	درصد فراوانی	تحصیلات	فراوانی	درصد فراوانی
استفاده از ابزار	کمتر از ۱ سال	۱ تا ۳ سال	۳ تا ۵ سال	بیشتر از ۵ سال	کل
فراوانی	۹	۷۸	۱۰۸	۹۷	۲۹۲
درصد فراوانی	۳/۱	۲۶/۷	۳۷	۳۳/۲	۱۰۰

شاخص‌های توصیفی متغیرهای پژوهش (جدول ۴) نشان می‌دهد که بیشترین میانگین مربوط به شدت تهدید درک‌شده (۳/۹۰) است. به بیان دیگر، هر نوع تهدیدی بر روی داده‌های دستگاه‌های الکترونیکی سیار پاسخ‌دهندگان مثل دانلودکردن برنامه‌های آلوده به ویروس، بیشترین تأثیر را روی دستگاه الکترونیکی سیار پاسخ‌دهندگان گذاشته است. کمترین میانگین مربوط به انگیزهٔ محافظت است و این یافته نشان می‌دهد که پاسخ‌دهندگان انگیزه‌ای برای محافظت از دستگاه خود در برابر تهدیدات نقض داده‌ها و اطلاعات دستگاه همراه خود ندارند و انگیزهٔ انجام فعالیت‌های مقابله‌ای در آن‌ها پایین است.

در این پژوهش جهت بررسی نرمال‌بودن توزیع متغیرها از دو شاخص چولگی و کشیدگی استفاده شد (جدول ۴). اگر مقدار شاخص چولگی برای هر متغیر در بازهٔ (۲+، ۲-) و مقدار شاخص کشیدگی در بازهٔ (۳+، ۳-) قرار داشته باشد، آن متغیر دارای توزیع نرمال است (Kline 2011). همان‌طور که مقدار عددی شاخص چولگی و کشیدگی (جدول ۴) نشان می‌دهد، تمامی متغیرها از توزیع نرمال پیروی می‌کنند.

جدول ٤. میانگین، انحراف معیار، چولگی و کشیدگی متغیرهای پژوهش

متغیر	میانگین	انحراف معیار	چولگی	کشیدگی
شدت تهدید درک‌شده	۳/۹۰	۰/۵۵	-۰/۴۰	۰/۲۰
حساسیت به تهدید درک‌شده	۳/۷۲	۰/۵۵	-۰/۴۴	۰/۸۱
هزینهٔ پاسخگویی درک‌شده	۳/۶۶	۰/۴۵	-۰/۵۶	۰/۴۸
اثربخشی پاسخ	۳/۳۹	۰/۵۴	-۰/۲۱	-۰/۰۸
خودکارآمدی	۳/۷۰	۰/۶۱	-۰/۲۳	-۰/۰۷
انگیزهٔ محافظت	۲/۹۵	۰/۶۶	-۰/۰۱	-۰/۱۷
استفاده از امنیت دستگاه	۳/۴۲	۰/۵۱	-۰/۲۸	۰/۲۶

۳-۲. یافته‌های استنباطی پژوهش

۳-۲-۱. ضریب همبستگی «پیرسون» بین متغیرهای پژوهش

ضریب همبستگی بین متغیرهای پژوهش (جدول ۵) نشان‌دهندهٔ رابطهٔ معنادار بین تمامی متغیرهاست.

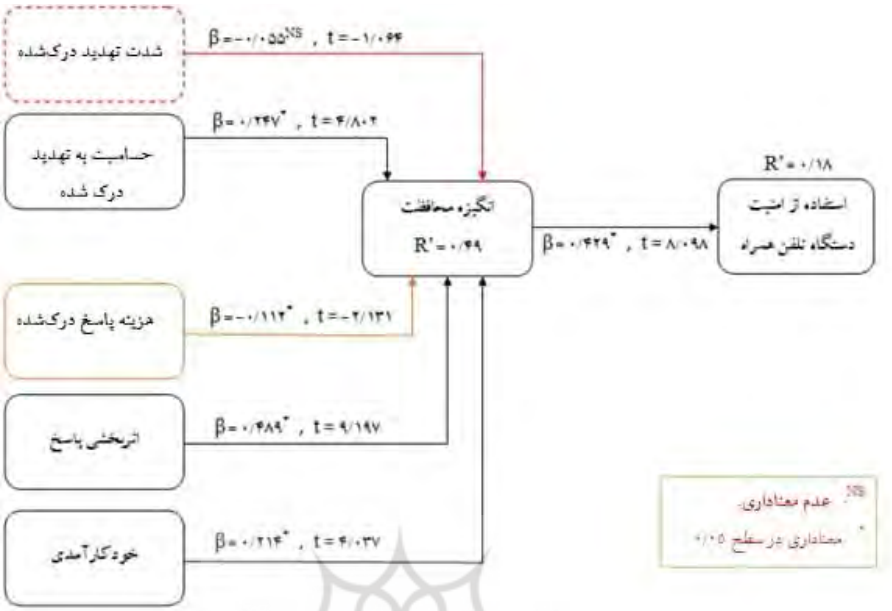
جدول ۵. ضریب همبستگی بین متغیرهای پژوهش

متغیرها	۱	۲	۳	٤	٥	٦	۷
شدت تهدید درک‌شده	۱						
حساسیت به تهدید درک‌شده	۰/۴۷۱**	۱					
هزینهٔ پاسخگویی درک‌شده	۰/۴۵۵**	۰/۳۴۲**	۱				
اثربخشی پاسخ	۰/۳۷۵**	۰/۳۶۰**	۰/۳۷۶**	۱			
خودکارآمدی	۰/۳۹۶**	۰/۲۴۸**	۰/۵۳۳**	۰/۳۵۱**	۱		
انگیزهٔ محافظت	۰/۲۹۵**	۰/۲۶۷**	۰/۲۶۰**	۰/۳۰۴**	۰/+۴۴**	۱	
استفاده از امنیت دستگاه	۰/۴۲۵**	۰/۳۱۴**	۰/۴۳۸**	۰/۳۲۹**	۰/۴۰۷**	۰/۴۲۹**	۱

**. معناداری در سطح ۰/۰۵

۳-۲-۲. برازش مدل

به‌منظور برازش مدل از مدل‌یابی معادلات ساختاری با به‌کارگیری روش حداقل مربعات جزئی در نرم‌افزار «آموس» استفاده شده است. شکل ۲، نتیجهٔ آزمون برازش مدل پژوهش و روابط ساختاری بین متغیرهای پژوهش را نشان می‌دهد.



شکل ۲. مدل ساختاری پژوهش در حالت تخمین استاندارد (مدل اصلی)

۳-۲-۳. آزمون فرضیه‌های پژوهش

نتایج آزمون فرضیه‌های پژوهش، با توجه به شکل ۲ و جدول ۵، به‌صورت زیر تفسیر می‌شود:

با توجه به ضریب مسیر و مقدار t ذکرشده در این رابطه (شکل ۲)، در سطح تشخیص ۰/۰۵ رابطه بین شدت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار مورد تأیید قرار نگرفت، زیرا آمارهٔ t داخل بازهٔ (۱/۹۶، ۱/۹۶-) قرار دارد. بنابراین، فرضیهٔ اول پژوهش مورد تأیید قرار نمی‌گیرد. به بیان دیگر، بین شدت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود ندارد. اما همان‌طور که مشاهده می‌شود (شکل ۲، جدول ۵)، در مورد رابطه بین حساسیت تهدید درک‌شده، هزینهٔ پاسخگویی درک‌شده، اثر بخشی پاسخ، خودکارآمدی با انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معناداری وجود دارد. بنابراین، فرضیهٔ دوم، سوم، چهارم و پنجم پژوهش مورد تأیید قرار می‌گیرد. با توجه به مثبت بودن علامت ضریب مسیر در مورد حساسیت تهدید درک‌شده، اثربخشی پاسخ، و خودکارآمدی می‌توان گفت این رابطه مثبت و مستقیم بوده و بین حساسیت تهدید درک‌شده، اثربخشی پاسخ و خودکارآمدی با

انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معنادار مستقیم وجود دارد. بنابراین، هر قدر حساسیت نسبت به تهدید احتمالی بیشتر باشد و مثلاً پاسخ‌دهندگان احتمال دهند که دستگاه تلفن همراه آن‌ها در اثر ویروس ممکن است خراب شود یا توسط یک هکر، هک شود و یا افراد اطمینان بیشتری پیدا کنند که اگر از نرم‌افزار ضد ویروس یا ضد بدافزار استفاده کنند، از دستگاه آن‌ها در برابر نقض داده‌ها و اطلاعات محافظت می‌شود و هر قدر افراد از انتخاب نرم‌افزار امنیتی و تنظیمات امنیتی مناسب و از نصب صحیح نرم‌افزارهای امنیتی بر روی دستگاه خود مطمئن باشند و به‌راحتی بتوانند اطلاعات مربوط به استفاده از نرم‌افزارهای امنیتی را در دستگاه تلفن همراه خود پیدا کنند، انگیزهٔ آن‌ها برای محافظت از ابزارهای الکترونیکی سیارشان افزایش می‌یابد. در همان حال، از آنجا که ضریب مسیر اثربخشی پاسخ نسبت به چهار متغیر دیگر بزرگ‌تر است، می‌توان گفت که تأثیر اثربخشی پاسخ در بالا بردن انگیزهٔ پاسخ‌دهندگان برای محافظت از ابزارهای الکترونیکی سیار بیشتر از بقیهٔ متغیرها خواهد بود.

اما چون علامت ضریب مسیر در مورد متغیر هزینهٔ پاسخگویی درک‌شده منفی است، بین هزینهٔ پاسخگویی درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار رابطهٔ معنادار غیر مستقیم وجود دارد. یعنی، افرادی که احساس می‌کنند برای نصب بدافزار یا ضد ویروس روی دستگاه همراه خود باید هزینه‌ای بپردازند و زمانی را صرف این کار بکنند، انگیزهٔ آن‌ها جهت محافظت از ابزارهای الکترونیکی سیارشان پایین می‌آید و شاید از این اقدام منصرف شوند.

یافته‌های پژوهش همچنین نشان داد که بین انگیزهٔ محافظت از ابزارهای الکترونیکی سیار و احتمال استفاده از امنیت ابزارهای الکترونیکی سیار رابطهٔ مثبت و معناداری وجود دارد. بنابراین، هر قدر انگیزهٔ پاسخ‌دهندگان برای محافظت از دستگاه تلفن همراه خود در برابر تهدیدات نقض داده‌ها و جلوگیری موفقیت‌آمیز از تهدیدات مربوط به نقض اطلاعات دستگاه همراه خود افزایش یابد، احتمال این‌که آن‌ها از امنیت ابزارهای الکترونیکی سیار خود استفاده کنند نیز افزایش می‌یابد.

جدول ۵. خلاصهٔ نتایج آزمون فرضیه‌های پژوهش

فرضیه	مسیر	ضریب مسیر	آمارهٔ t	سطح معناداری	نتیجه
۱	شدت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار	-۰/۰۵۵	-۱/۰۶۴	۰/۲۸۷	رد
۲	حساسیت تهدید درک‌شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار	۰/۲۴۷	۴/۸۰۲	۰/۰۰۱	تأیید
۳	هزینهٔ پاسخگویی درک شده و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار	-۰/۱۱۲	-۲/۱۳۱	۰/۰۰۱	تأیید
۴	اثر بخشی پاسخ و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار	۰/۴۸۹	۹/۱۹۷	۰/۰۰۱	تأیید
۵	خودکارآمدی و انگیزهٔ محافظت از ابزارهای الکترونیکی سیار	۰/۲۱۴	۴/۰۳۷	۰/۰۳۳	تأیید
۶	انگیزهٔ محافظت و احتمال استفاده از امنیت ابزارهای الکترونیکی سیار	۰/۴۲۹	۸/۰۹۸	۰/۰۰۱	تأیید

٤. بحث و نتیجه‌گیری

از آنجا که امروزه موارد مربوط به نقض داده‌ها و آسیب‌پذیری امنیت اطلاعات رواج بیشتری یافته (Xu et al. 2019) و این مسئله می‌تواند صدمات جبران‌ناپذیر مادی و معنوی بر کاربران ابزارهای الکترونیکی سیار وارد نماید، مطالعه بر روی جنبه‌های مختلف آن از اهمیت وافری برخوردار است. از این رو، در این پژوهش بر اساس نظریهٔ انگیزهٔ محافظت از نقض داده‌ها، رفتار تجربی دانشجویان تحصیلات تکمیلی دانشگاه «ایلام» هنگام استفاده از ابزارهای الکترونیکی سیار (موبایل، لپ‌تاپ، تبلت) مورد بررسی قرار گرفت.

بر اساس یافته‌های پژوهش حاضر، شدت تهدید درک‌شده بر انگیزهٔ محافظت تأثیر معناداری ندارد. این بخش از یافته‌ها با نتایج پژوهش Giwah (2019) همخوانی دارد، اما با یافته‌های Vance, Siponen & Pahnila (2012)، Herath, & Rao (2009)، Claar & Johnson (2012) و Posey, Roberts & Lowry (2015) همسو نیست. عدم همخوانی این یافته با یافته‌های پژوهش‌های قبلی شاید به این دلیل است که جامعهٔ هدف این پژوهش دانشجویان هستند و این افراد با پیشرفت‌های تکنولوژیکی کم‌وبیش آشنا بوده و از اعتمادبه‌نفس بالایی در هنگام استفاده از ابزارهای الکترونیکی سیار برخوردارند و به احتمال، به اثربخشی و خودکارآمدی دستگاه الکترونیکی خود برای محافظت از داده‌ها اطمینان دارند. شاید به همین خاطر است که آن‌ها شدت تهدیدات درک‌شده را جدی نمی‌گیرند و شدت

تهدیدات درک‌شده انگیزهٔ محافظت آن‌ها هنگام استفاده از دستگاه الکترونیکی سیار را تحریک نمی‌کند.

افزون بر این، پژوهش حاضر نشان داد که حساسیت به تهدید درک‌شده، انگیزهٔ محافظت دانشجویان را تحت تأثیر مثبت قرار داده و آن را تحریک می‌کند. بدیهی است که کاربران دستگاه‌های الکترونیکی سیار حساسیت به تهدید را یک عامل ضروری بدانند و باعث شود آن‌ها بخواهند اقدامات امنیتی انجام دهند که از دستگاه‌های خود در برابر نقض داده‌ها محافظت کند. این یافته شگفت‌آور نیست، زیرا برخی از پژوهش‌های قبلی (مانند Giwah 2019؛ Dang-Pham & Pittayachawan 2015؛ Posey et al. 2015؛ Herath and Rao 2009) نیز از این یافته حمایت می‌کنند. همهٔ این پژوهشگران نتیجه گرفتند که کاربران در صورت حساسیت به تهدیدات، انگیزه پیدا می‌کنند تا از خود محافظت کنند و درک آسیب‌پذیر بودن در معرض تهدید منجر به شناسایی ارزیابی‌های مقابله‌ای می‌شود و به کاربران انگیزه می‌دهد که از خود محافظت کنند. در تبیین این یافته می‌توان گفت که از جملهٔ تهدیدهایی که ممکن است دانشجویان نسبت به آن حساسیت داشته باشند، عبارت است از: خراب شدن و از بین رفتن اطلاعات روی دستگاه سیار در اثر حملهٔ ویروس از طریق برنامه‌های آلوده به ویروس، و هک شدن و به سرقت رفتن اطلاعات مهم شخصی (حساب بانکی، تأمین اجتماعی و غیره) از دستگاه.

همچنین، یافته‌های این پژوهش نشان داد که اثربخشی پاسخ نیز انگیزهٔ محافظت را در جهت مثبت تحریک می‌کند. یافته‌های Giwah (2019)، Posey, Roberts & Lowry (2015)، Vance, Siponen & Pahnila (2012)، Johnston & Warkentin (2010)، Herath and Rao (2009) و Davis, Bagozzi & Warshaw (1989) نیز این یافته را تأیید می‌کنند. در تبیین این یافته می‌توان گفت که وقتی دانشجویان متوجه شوند، نرم‌افزاری (مانند ضد ویروس یا ضد بدافزار) وجود دارد که اگر آن را نصب کنند از دستگاه سیار آن‌ها در برابر نقض داده‌ها محافظت خواهد کرد، انگیزهٔ محافظت در آن‌ها تحریک خواهد شد.

همانند یافته‌های مطالعات قبلی، مانند Vance, Siponen & Pahnila (2012) و Herath and Rao (2009)، نتایج حاصل از این مطالعه نیز نشان داد که هزینهٔ پاسخگویی درک‌شده اقدامات امنیتی، بر انگیزهٔ محافظت دانشجویان از دستگاه‌های الکترونیکی سیار برای ایمن‌سازی دستگاه‌های خود در برابر نقض داده‌ها تأثیر منفی می‌گذارد. اما این یافته‌ها با یافته‌های Giwah (2019) در این زمینه همخوان نیست. این عدم همخوانی به احتمال، به این دلیل است که جامعهٔ هدف در پژوهش او به اثربخشی پاسخ و خودکارآمدی

دستگاه تلفن همراه بیشتر از هزینهٔ پاسخ درک‌شده اهمیت می‌دهند. از یافته‌های مطالعهٔ Giwah (2019) می‌توان نتیجه گرفت که هنگامی که کاربرانِ ابزارهای الکترونیکیِ سیار به کارایی پاسخ و عدم کارایی دستگاه همراه در برابر تهدیدات امنیتی بسیار اطمینان دارند، هزینهٔ پاسخ درک‌شده آن‌ها تأثیر معناداری بر رفتار امنیتی محافظ آن‌ها ندارد. به بیان دیگر، کاربران به خودکارآمدی و اثربخشی پاسخ بیشتر از هزینهٔ پاسخ درک‌شده اهمیت می‌دهند؛ در حالی که در پژوهش حاضر این‌طور نیست و هزینهٔ پاسخ درک‌شده باعث کم‌شدن انگیزهٔ محافظت دانشجویان هنگام استفاده از ابزارهای الکترونیکی سیار خود در برابر نقض داده می‌شود.

طبق گفته‌های Boss et al. (2015) و Posey, Roberts & Lowry (2015) در فرایند ارزیابی مقابله‌ای نظریهٔ انگیزهٔ محافظت، اثربخشی پاسخ و خودکارآمدی باید بیش از هزینهٔ پاسخگویی باشد تا فرد درگیر انگیزهٔ محافظت شود. از یافته‌های مطالعهٔ Giwah (2019)، مشخص است که اثربخشی پاسخ و خودکارآمدی دستگاه تلفن همراه کاربران دستگاه‌های تلفن همراه از هزینهٔ پاسخگویی درک‌شدهٔ خود برای مشارکت در رفتار محافظتی فراتر رفته است. بنابراین، یافته‌های او نشان داد که وقتی کاربران دستگاه‌های تلفن همراه به کارایی پاسخ در برابر تهدیدات امنیتی اطمینان دارند، هزینهٔ پاسخگویی درک‌شدهٔ آن‌ها تأثیر معناداری بر رفتار امنیتی محافظ آن‌ها ندارد و آن‌ها به خودکارآمدی و اثربخشی پاسخ، بیشتر از هزینهٔ پاسخگویی درک‌شده اهمیت می‌دهند. این در حالی است که در پژوهش حاضر هزینهٔ پاسخگویی درک‌شده باعث کم‌شدن انگیزهٔ محافظت دانشجویان هنگام استفاده از دستگاه‌های الکترونیکی سیار در برابر نقض داده‌ها می‌شود. در تبیین این یافته می‌توان گفت که با توجه به این‌که زمان یکی از هزینه‌های مد نظر این پژوهش است، بعضی اوقات استفاده‌کردن از نرم‌افزار ضد ویروس و ضد بدافزار در دستگاه الکترونیکی سیار، راحتی استفاده از دستگاه را کاهش داده و گاهی باعث کند شدن سرعت عملکرد آن می‌شود؛ حتی نصب نرم‌افزار بر روی دستگاه در بعضی مواقع زمان زیادی را به خود اختصاص می‌دهد. همین امر باعث از دست رفتن انگیزهٔ نصب برای استفاده از این نرم‌افزارها می‌شود. افزون بر این، برخی از این نرم‌افزارها هزینه‌بر است و از آنجا که جامعهٔ آماری پژوهش حاضر را دانشجویان تشکیل می‌دهند و این قشر به‌طور معمول از لحاظ مالی در وضعیت مناسبی قرار ندارند، به احتمال، از استفاده از این نرم‌افزارها صرف نظر می‌کنند و خطر نقض دادهٔ دستگاه تلفن همراه خود را می‌پذیرند.

یافته‌ها همچنین نشان داد که خودکارآمدی دستگاه‌های الکترونیکی سیار به میزان قابل توجهی بر انگیزهٔ افراد برای محافظت از دستگاه خود در برابر نقض اطلاعات، تأثیرگذار است. این یافته نیز با یافته‌های پژوهش‌های قبلی (مانند Giwah 2019؛ Herath and Rao 2009؛ Vance, Siponen & Pahnila 2012؛ Johnston and Warkentin 2010؛ Kim, Yang & Park 2014؛ Posey, Roberts & Lowry 2015) همخوانی دارد. «چان، وون و کانکانالی» در این زمینه خاطرنشان کردند که عدم کارایی تلفن همراه باعث خواهد شد که کاربران آن قصد داشته باشند که از دستگاه‌های خود محافظت کنند (Chan, Woon & Kankanhalli 2005). در تبیین این یافته می‌توان گفت که وقتی دانشجویان نحوهٔ نصب نرم‌افزار امنیتی مناسب روی دستگاه خود را خوب یاد بگیرند و از نصب صحیح آن روی دستگاه خود اطمینان داشته باشند و بدانند که چطور تنظیمات امنیتی مناسبی را برای دستگاه خود انتخاب کنند، انگیزهٔ آن‌ها برای محافظت از دستگاه در مقابل نقض اطلاعات افزایش می‌یابد و در این راستا اقدامات لازم را انجام خواهند داد.

در انتها، نتایج به‌دست‌آمده از تجزیه و تحلیل داده‌ها در پژوهش حاضر نشان داد که میزان استفادهٔ دانشجویان از امنیت ابزارهای الکترونیکی سیار خود به‌طور قابل توجهی تحت تأثیر انگیزهٔ آن‌ها برای محافظت از این دستگاه‌ها در برابر نقض داده‌هاست. ادبیات موجود در این زمینه کاملاً از این یافته پشتیبانی می‌کند و این یافته با یافته‌های Giwah (2019) و Posey, Roberts & Lowry (2015) همخوانی دارد. از این گذشته، در این مورد «جانستون و وارکنتین» با استناد به Rogers (1983) ادعا کردند که وقتی ارزیابی تهدید و ارزیابی‌های مقابله‌ای در سطح متوسط تا بالا باشد، انگیزهٔ محافظت فردی به همان اندازه افزایش می‌یابد و از این رو، بر رفتار واقعی تأثیر می‌گذارد (Johnston and Warkentin 2010). «راجرز» نیز اظهار داشت که انگیزهٔ محافظت متغیری است که باعث تغییر رفتار می‌شود (Rogers 1983). در تبیین این یافته می‌توان گفت که وقتی دانشجویان برای جلوگیری موفقیت‌آمیز از تهدیدات مربوط به نقض اطلاعات دستگاه همراه خود انگیزهٔ انجام فعالیت‌های مقابله‌ای را داشته و بی‌تفاوت نباشند، خودبه‌خود دنبال راه چاره می‌گردند و نخست، به تنظیمات دستگاه همراه خود سر می‌زنند و سعی می‌کنند تا جایی که امکان داشته باشد از امکانات دستگاه استفاده کنند. به‌عنوان مثال، آن‌ها برای محافظت از دستگاه سیار خود از رمز عبور و یا از حفاظت بیومتریک استفاده می‌کنند یا اقدام به روزآمدسازی سیستم‌عامل و نرم‌افزارهای دستگاه کرده یا از روش تهیهٔ نسخهٔ پشتیبان،

محافظ فایروال و نصب نرم‌افزار آنتی‌ویروس روی ابزارهای الکترونیکی سیار خود استفاده می‌کنند و از این طریق از امنیت دستگاه همراه خود مطمئن می‌شوند.

به‌طور کلی، پژوهش حاضر نشان داد که شدت تهدید درک‌شده، انگیزهٔ محافظت کاربران دستگاه‌های الکترونیک سیار را تحریک نمی‌کند، اما سازه‌های حساسیت به تهدید درک‌شده، اثربخشی پاسخ و خودکارآمدی ابزارهای الکترونیکی سیار و هزینهٔ پاسخگویی درک‌شده بر انگیزهٔ محافظت تأثیر دارد و انگیزهٔ محافظت نیز بر استفاده از امنیت این دستگاه‌ها تأثیر مثبت دارد. از طرفی، هزینهٔ پاسخ درک‌شده باعث کم‌شدن انگیزهٔ محافظت دانشجویان هنگام استفاده از ابزارهای الکترونیکی سیار خود در برابر نقض داده می‌شود و ارزیابی کاربران از حساسیت‌های خود در برابر تهدیدات و میزان اعتماد به توانایی‌های خودشان در جهت استفادهٔ مناسب از امکانات امنیتی ابزارهای الکترونیکی سیار و خودکارآمدی دستگاه‌ها و اثربخشی پاسخ، تعیین‌کنندهٔ میزان انگیزهٔ آنان برای انجام اقدامات محافظتی است و افزایش یا کاهش انگیزهٔ محافظت، تعیین‌کنندهٔ میزان استفاده از امنیت ابزارهای الکترونیکی سیار است. در کل، این پژوهش و بسیاری از پژوهش‌های قبلی (مثل Giwah 2019؛ Posey, Roberts & Lowry 2015؛ Milne, Sheeran & Orbell 2000؛ Rippetoe & Rogers 1987) بر این نکته تأکید دارند که فرایند ارزیابی مقابله‌ای عامل مهم‌تری نسبت به فرایند ارزیابی تهدید در افزایش انگیزهٔ محافظت کاربران است.

۵. پیشنهاد پژوهش

گسترهٔ پژوهش در حوزهٔ امنیت داده‌ها در وسایل الکترونیکی از قبیل گوشی‌های هوشمند، تبلت‌ها و ... که کاربران به‌صورتی روزافزون از آن استفاده می‌کنند، بسیار وسیع است و پژوهش‌ها در ایران چندان به این مبحث نپرداخته‌اند. بر اساس نتایج پژوهش حاضر، از آنجا که استفاده از امنیت ابزارهای الکترونیکی سیار مبتنی بر رفتار شخصی کاربران است و فرایند ارزیابی مقابله‌ای به نسبت ارزیابی تهدید، عامل مهم‌تری در افزایش انگیزهٔ محافظت از سوی کاربران است، پیشنهاد می‌شود هنگام روزآمدسازی ابزارهای الکترونیکی سیار به این مهم توجه شده و تمهیداتی در این زمینه، چه از نظر سخت‌افزاری و چه از لحاظ نرم‌افزاری در نظر گرفته شود. همچنین، لازم است تولیدکنندگان ابزارهای الکترونیکی سیار از طریق برنامه‌های آگاهی‌رسانی، بیشتر بر جنبه‌های روان‌شناختی رفتار کاربران متمرکز شوند تا بتوانند رفتار امنیت اطلاعات را در کاربران تقویت نمایند.

فهرست منابع

پیکری، حمیدرضا، و بابک بنازاده. ۱۳۹۷. رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت، *پژوهش‌های راهبردی مسائل اجتماعی ایران* ۲۳ (۴): ۴۱-۵۸.

حسینی دوزین، خدیجه. ۱۳۹۵. رفتار امنیتی اطلاعات کاربران گوشی‌های هوشمند بر اساس نظریهٔ تجزیه‌یافتهٔ رفتار برنامه‌ریزی‌شده. پایان‌نامهٔ کارشناسی‌ارشد، دانشگاه بیرجند، دانشکدهٔ علوم تربیتی و روان‌شناسی.

حسینی سنو، سید امین، و الهام مظاهری. ۱۳۹۷. تأثیر حریم خصوصی، امنیت و اعتماد ادراک‌شده بر رفتار به اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی موبایل؛ نقش تعدیل‌کننده متغیر جنسیت. پژوهشنامه پردازش و مدیریت اطلاعات ۳۴ (۱): ۲۴۵-۲۷۴.

خارا، روح‌الله، و مرضیه صارمیان. ۱۳۹۴. مروری جامع بر خطرات تهدیدکنندهٔ اطلاعات سلامت در ابزارهای سیار. *مجله انفورماتیک سلامت و زیست‌پزشکی، مرکز تحقیقات انفورماتیک پزشکی* ۲ (۱): ۴۸-۵۶.

کریمی، زهرا، و حمیدرضا پیگری. ۱۳۹۷. تأثیر ادراک پرستاران از آموزش امنیت اطلاعات و آگاهی از سیاست‌های امنیت اطلاعات بر ادراک از شدت و قطعیت مجازات نقض امنیت اطلاعات. *نشریه آموزش پرستاری* ۷ (۲): ۵۵-۶۷.

محمودزاده، ابراهیم، و مهدی رادرجبی. ۱۳۸۵. مدیریت امنیت در سیستم‌های اطلاعاتی. *فصلنامه علوم مدیریت ایران* ۱ (۴): ۷۸-۱۱۲.

References

Anderson, C. L., & R. Agarwal. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intention. *MIS Quarterly* 34 (3): 613-643.

Boss, S., D. F. Galletta, P. B. Lowry., G. D. Moody & P. Polak. 2015. What do users have to fear? Using fear appeals to engender threats and fear that security behaviors motivate protective. *MIS Quarterly* 39 (4)864–837 :.

Chan, M., I. Woon, & A. Kankanhalli. 2005. Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security* 1 (3): 18-41.

Claar, C. L., & J. Johnson. 2012. Analyzing home PC security adoption behavior. *Journal of Computer Information Systems* 52 (4): 20-29.

Crismaru M. 2006. Using protection motivation theory to increase the persuasiveness of public service communications. *SIPP public policy* 40 (9): 545-556.

Dang-Pham, D., & S. Pittayachawan. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. *Computers & Security* 48 (2): 281-297.

Davis, F. D., R. P. Bagozzi, & P. R. Warshaw. 1989. User acceptance of computer technology: a comparison of two theoretical models. *Management Science* 35 (8): 982-1003.

Douglas, D. M. 2019. Should researchers use data from security breaches? *Communications of the ACM* 62 (12): 22-24.

Floyd, D. L., S. Prentice-Dunn & R. W. Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30 (2): 407-429.

Giwah, A. D. 2019. Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and computing. (1073) https://nsuworks.nova.edu/gscis_etd/1073 (accessed March 3, 2020)

_____, L. Wang, Y. Levy & I. Hur.2020 . Empirical assessment of mobile device users' information security behavior towards data breach. *Journal of Intellectual Capital* 21 (2): 215-233.

Herath, T., & H. R. Rao. 2009. Protection motivation and deterrence: a framework for Security policy compliance in organizations. *European Journal of Information Systems* 18 (2): 106-125.

Ifinedo, P. 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31 (1): 83– 95.

Johnston, A. C., & M. Warkentin. 2010. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* 34 (3): 549-566.

Kim, S. H., K. H. Yang, & S. Park. 2014. An integrative behavioral model of information security policy compliance. *The Scientific World Journal* 12 (4): 548-655.

Kline, R. B. 2011. *Principles & Practice of Structural Equation Modeling. Second Edition*,. New York: The Guilford Press.

Milne, S., P. Sheeran, & S. Orbell. 2000. Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology* 30 (1): 106-143.

Mousavi, R., R. Chen, D. J. Kim, & K. Chen. 2020. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems* 135: 1-14 https://doi.org/10.1016/j.dss.2020.113323.

Posey, C., T. L. Roberts, & P. B. Lowry. 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32 (4): 179-214.

Park, E., J. Kim, & Y. S. Park. 2017 The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information. *Computers & Security* 65 (4): 64-76.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology* 91 (1): 93-114.

Rogers, R. W. 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

Rippetoe, P. A., & R. W. Rogers. 1987. Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology* 52: 596–604.

Vance, A., M. Siponen, & S. Pahnila. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management* 49 (3-4): 190-198.

Veiga. A., & N. Martins. 2017. Defining and Identifying Dominant Information Security Cultures and Subcultures. *Computers & Security* 70 (4): 72-94.

Woon, Irene, Tan Gekwood, and R. Low. 2005. A Protection Motivation Theory Approach to Home Wireless Security. ICIS 2005 Proceedings. 31. https://aisel.aisnet.org/icis2005/31 (accessed March 3, 2020)

Xu, H., S. Guo, J. Z. Haislip& R. E. Pinsker. 2019. Earnings management in firms with data security breaches. *Journal of Information Systems* 33 (3): 267-284.

فرامرز سهیلی

متولد سال ۱۳۵۶، دارای مدرک دکتری علم اطلاعات و دانش‌شناسی از دانشگاه شهید چمران اهواز است. ایشان هم‌اکنون دانشیار گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور است.

علم‌سنجی، اطلاع‌سنجی، وب‌سنجی، جامعه‌شناسی علم و رفتار اطلاعاتی از جمله علایق پژوهشی وی هستند

رضا روستایی

متولد سال ۱۳۶۹، دارای مدرک تحصیلی کارشناسی ارشد در رشتهٔ علم اطلاعات و دانش‌شناسی، مطالعات کتابخانه‌های عمومی از دانشگاه پیام نور استان کرمانشاه است.

رفتار اطلاعاتی، ابزارهای الکترونیکی از علایق پژوهشی وی است.

علی‌اکبر خاصه

متولد سال ۱۳۶۰، دارای مدرک دکتری علم اطلاعات و دانش‌شناسی است. ایشان هم‌اکنون دانشیار گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور است.

علم‌سنجی از جمله علایق پژوهشی وی است.

مهری شهبازی

متولد سال ۱۳۵۱، دارای مدرک تحصیلی دکتری در علم اطلاعات و دانش‌شناسی از دانشگاه شهید چمران اهواز است. ایشان هم‌اکنون استادیار گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور است.

نظام‌های اطلاعاتی، مدیریت دانش و سازماندهی، کتابداری واطلاع‌رسانی برای کودک و نوجوان از جمله علایق پژوهشی وی است.