Journal of Innovation in Sports Management
Volume 2, Issue 2, Summer 2023;155-168
https://jism.srbiau.ac.ir/

Investigating the Mediating Role of Stubbornness in the Relationship between Habit and Intention of Cyber Security Behavior in Physical Education Teachers of South Khorasan Province

Kazem Chirag Birjandi — Assistant Professor, Department of Physical Education, Birjand Branch, Islamic Azad University, Birjand, Iran

Fateme Hamidi — Master's student in sports management, Birjand Branch, Islamic Azad University, Birjand, Iran

Fateme Sheikhi Molashahi — Master's student in sports management, Birjand Branch, Islamic Azad University, Birjand, Iran

Fateme Alidoost — Master's student in sports management, Birjand Branch, Islamic Azad University, Birjand, Iran

Original Research Articel

Received: 2023-16-04

Accepted: 2023-18-05

Abstract

The aim of the present study was to investigate the mediating role of stubbornness in the relationship between habit and intention of cyber security behavior in physical education teachers of South Khorasan province. The research method was descriptive and was conducted in the field. The statistical population of the research included all physical education teachers of South Khorasan province, 267 people in the academic year of 1402-1401. According to Morgan's table, the sample was selected as 152 people, and random sampling method was used. The research tools included 3 standard habit questionnaires of Siponeh et al. (2012), Barton's standard stubbornness questionnaire (2000) and Thompson et al.'s cyber security behavior intention questionnaire (2017) were used. To ensure the reliability of the questionnaires, 30 copies were distributed in the preliminary study on the sample(s) that were completely randomly selected, and Cronbach's alpha coefficient for the habit questionnaire (α=0.89), stubbornness questionnaire (α=0.84) , and for the cyber security behavior intention questionnaire (α=0.79) was obtained. The results of the research showed that stubbornness plays a mediating role in the relationship between habit and intention of cyber security behavior in physical education teachers of South Khorasan province. According to the research results, it is suggested; Paying attention to cyber security behaviors in educational environments, including schools, should be paid attention to by administrators and teachers, and for this reason, they should not neglect individual behavioral characteristics and habits to facilitate dealing with cyber actions.

Key words: Habit, Stubbornness, Physical Education, Teachers, Security Behavior

∗ Corresponding Author: kbirjandi@iaubir.ac.ir

How to Cite: Chirag Birjandi K, Hamidi F, Sheikhi Molashahi F, Alidoost F. Investigating the Mediating Role of Stubbornness in the Relationship between Habit and Intention of Cyber Security Behavior in Physical Education Teachers of South Khorasan Province, Journal of Innovation in Sports Management, 2023;2(2):155-168.

نوآوری در مدیریت ورزشی
دوره ۲، شماره ۲، تابستان ۱۴۰۲،
۱۶۸-۱۵۵
https://jism.srbiau.ac.ir/

مقاله پژوهشی

تاریخ دریافت: ۱۴۰۲/۰۱/۲۷
تاریخ پذیرش: ۱۴۰۲/۰۲/۲۸

بررسی نقش میانجی سرسختی در ارتباط عادت با قصد رفتار امنیتی سایبری در معلمان تربیت بدنی استان خراسان جنوبی

کاظم چراغ بیرجندی | استادیار گروه تربیت بدنی، واحد بیرجند، دانشگاه آزاد اسلامی، بیرجند، ایران
فاطمه حمیدی | دانشجوی کارشناسی ارشد مدیریت ورزش، واحد بیرجند، دانشگاه آزاد اسلامی، بیرجند، ایران
فاطمه شیخی ملاشاهی | دانشجوی کارشناسی ارشد مدیریت ورزش، واحد بیرجند، دانشگاه آزاد اسلامی، بیرجند، ایران
فاطمه علیدوست | دانشجوی کارشناسی ارشد مدیریت ورزش، واحد بیرجند، دانشگاه آزاد اسلامی، بیرجند، ایران

چکیده

هدف: هدف از پژوهش حاضر، بررسی نقش میانجی سرسختی در ارتباط عادت با قصد رفتار امنیتی سایبری در معلمان تربیت بدنی استان خراسان جنوبی بود. روش تحقیق از نوع توصیفی بود و به شکل میدانی انجام‌شد. جامعه آماری پژوهش شامل کلیه معلمان تربیت بدنی استان خراسان جنوبی به تعداد ۲۶۷ نفر سال تحصیلی ۱۴۰۲-۱۴۰۱ بودند. نمونه با توجه به جدول مورگان به تعداد ۱۵۲ نفر انتخاب شدند که شیوه نمونه گیری به صورت تصادفی استفاده شد. ابزار پژوهش شامل ۳ پرسشنامه استاندارد عادت سیپونه و همکاران (۲۰۱۲)، پرسشنامه استاندارد سرسختی بارتون (۲۰۰۰) و پرسشنامه قصد رفتارهای امنیت سایبری تامپسون و همکاران (۲۰۱۷) مورد استفاده قرار گرفتند. برای اطمینان از پایایی پرسشنامه‌ها ۳۰ نسخه آن در مطالعه مقدماتی بر روی نمونه(ها) که به‌طور کاملاً تصادفی انتخاب‌شده بود، توزیع شد و ضریب آلفای کرونباخ برای پرسشنامه عادت (α=۰/۸۹)، پرسشنامه سرسختی (α=۰/۸۴) ، و برای پرسشنامه قصد رفتارهای امنیت سایبری (α=۰/۷۹) بدست آمد. نتایج تحقیق نشان داد سرسختی در ارتباط عادت با قصد رفتار امنیتی سایبری در معلمان تربیت بدنی استان خراسان جنوبی نقش میانجی دارند. با توجه به نتایج پژوهش پیشنهاد می شود؛ توجه به رفتارهای امنیتی سایبری در محیط های آموزشی از جمله مدارس موراد توجه مدیران و معلمان قرار گیرد و برای این مهم از ویزگی های رفتاری و عادت ها فردی در جهت تسهیل مقابله با اقدامات سایبری غافل نباشند.

* **نویسنده مسئول:** kbirjandi@iaubir.ac.ir

چراغ بیرجندی کاظم، حمیدی فاطمه، شیخی ملاشاهی فاطمه، علیدوست فاطمه، بررسی نقش میانجی سرسختی در ارتباط عادت با قصد رفتار امنیتی سایبری در معلمان تربیت بدنی استان خراسان جنوبی، فصلنامه نوآوری در مدیریت ورزشی، تابستان ۱۴۰۲، ۲(۲): ۱۶۸-۱۵۵

واژگان کلیدی: عادت، سرسختی، تربیت بدنی، معلمان، رفتار امنیتی

مقدمه

عصری که در آن زندگی میکنیم را میتوان عصر سایبری نام نهاد. از آن جهت که فناوریهای نوین ارتباطی در زندگی و جامعه مدرن کنونی، نقش و جایگاهی بیبدیلی را به خود اختصاص دادهاند تا جاییکه تصور جامعه معاصر بدون آنها، بسیار دشوار به نظر میرسد، در حال حاضر شاهد شکل گیری فضایی هستیم که در آن فعالیتهای گوناگونی مانند اطلاع رسانی، ارائه خدمات، مدیریت وکنترل ارتباطات، از طریق سازوکارهای فضای سایبری انجام می پذیرد (بلوردی و طیاری، ۱۴۰۱: ۶۵). از این رو مفهوم امنیت سایبری موضع مهم و نو در این حوزه است. امنیت سایبری مجموعه ابزارها، سیاستها، مفاهیم امنیتی، اعمال امنیتی، رویکردهای مدیریت بحران، اعمال، آموزش و فناوریهای می باشد که در راستای در دسترس بودن، مورد اطمینان بودن و صحت اطلاعات میباشد که به منظور حفاظت از محیط اسایبری و دارایی کاربران و سازمانها به کار می رود .انسان ها بزرگترین تهدید و ضعیف ترین حلقه در امنیت سایبری هستند (صفا[1] و همکاران،۲۰۱۹، ۵۹۰). مطالعات نشان دادهاند که اگرچه اقدامات کارکنان ممکن است تهدیدات امنیتی، خطرات و آسیب‌پذیری‌ها را به همراه داشته باشد (آیگفو[2] و همکاران، ۲۰۲۰ ،۱۱۵)، کارکنان نیز اولین خط دفاعی سازمان برای مقابله و کاهش تهدیدات امنیت سایبری هستند. مجرمان سایبری می‌دانند که ساده‌ترین راه برای دسترسی به سیستم‌های اطلاعاتی یک سازمان، از طریق ضعیف‌ترین حلقه، اغلب کارمندان است. در سال ۲۰۱۸، ۵۳ درصد از شرکت‌های کوچک و متوسط[3] با نقض داده‌ها، از جمله حملات فیشینگ[4] هدفمند، علیه کارکنان خود مواجه شدند. بنابراین، رفتار امنیتی کارکنان یک نگرانی اصلی است (سیسکو[5]، ۲۰۱۸، ۲۵). مجرمان سایبری اغلب از طریق ضعف های امنیتی در شبکه های زنجیره تامین SME به داده های سازمان های بزرگتر و دولت دسترسی پیدا می کنند(کی پی ام جی[6]، ۲۰۱۸ ،۳۰) . فقدان منابع، دانش و سرمایه‌گذاری کم شرکت‌های کوچک و متوسط در امنیت دیجیتال برای مجرمان سایبری به خوبی شناخته شده است و توضیح می‌دهد که چرا شرکت‌های کوچک و متوسط و کارکنان آن‌ها به طور فزاینده‌ای مورد هدف قرار می‌گیرند(ورزن[7]،۲۰۱۹ ،۴۰). تحقیقات قبلی عواملی را شناسایی کرده‌اند که ممکن است بر قصد کارمند برای پیروی از سیاست‌ها و رویه‌های امنیتی تأثیر بگذارد(هرس[8] و همکاران،۲۰۱۸ ،۱۱۰). با این حال، بخش عمده ای از این مطالعات در سازمان های بزرگ انجام شده است که در آن سلسله مراتب سازمانی با سیاست های رسمی امنیت اطلاعات که با استفاده از استانداردهای امنیتی بین المللی ایجاد شده اند وجود دارد(فلوردی و تیکز[9]،۲۰۱۶،۱۷۵)

1 Safa
2 Aigbefo
3 SMEs
4 Phishing
5 Cisco
6 KPMG
7 Verizon
8 Herath
9 Flowerday and Tuyikeze

تحقیقات نشان می‌دهد که برخی ویژگی‌های سازمانی مانند اندازه، صنعت و درآمد بر اثربخشی مدیریت امنیت اطلاعات تأثیر می‌گذارند (میجن و همکاران[1]، ۲۰۱۶، ۲۱).

تحقیقات گذشته در مورد امنیت اطلاعات رفتاری عواملی را بررسی می‌کند که قصد رفتار منطبق بر کارمندان را با توجه به سیاست‌ها و رویه‌های امنیتی ارتقا می‌دهد. این عوامل دو دیدگاه انگیزشی دارند: بیرونی و درونی. دیدگاه بیرونی، که بیشتر ادبیات امنیت اطلاعات رفتاری تحت آن قرار می‌گیرد، شامل عوامل ملموسی است که سازمان‌ها برای تأثیرگذاری بر قصد رفتار کارکنان برای پیروی از رویه‌های امنیتی، به عنوان مثال، تأثیرگذاری بر رفتار امنیتی کارکنان از طریق اقدامات متقابلی مانند سیاست‌های امنیتی، نرم‌افزار، و آموزش امنیت آگاهی از امنیت اطلاعات؛ اجرای پاداش ها، تحریم ها و مجازات ها، یا استفاده از پیام های ترس (آگبفو و همکاران، ۲۰۲۰، ۱۱۷). از سوی دیگر دیدگاه ذاتی شامل عوامل نامشهودی است که مختص یک فرد است. مطالعات در مقوله ذاتی توضیحاتی را برای ویژگی‌های روحی و روانی ارائه می‌دهند که بر قصد رفتار امنیتی تأثیر می‌گذارند، مانند عادت، شخصیت (گراتیان[2] و همکاران ۲۰۱۸، ۳۵۰) و منابع روانشناختی (برنز[3] و همکاران ۲۰۱۷، ۵۱۲). کارکنان به طور فزاینده ای به عنوان بخشی از راه حل برای کاهش تهدیدات امنیتی شناخته می شوند، به ویژه هنگامی که منابع روانی مناسب را توسعه می دهند(فارنل[4] و همکاران، ۲۰۱۸، ۵).

برای محدود کردن رفتار انحرافی، سازمان‌ها اغلب مکانیسم‌های(سازوکارهای) تحریم(محرومیت یا مجازات) رسمی یا غیررسمی را اجرا می‌کنند (چن[5] و همکاران ۲۰۱۸، ۱۰۵۵). یک متاآنالیز[6] از اثربخشی مکانیسم‌های(سازوکارهای) تحریم که شدت تحریم، قطعیت تحریم و شفافیت تحریم را بررسی می‌کند، همبستگی مثبتی را برای این سه سازه بازدارنده پیدا کرد(ترانگ[7]، ۲۰۱۸، ۱۷). تحقیقات همچنین رویکردهایی را برای مهار رفتار انحرافی از طریق مکانیسم‌های پاسخگویی، یعنی قابلیت شناسایی، آگاهی از ثبت گزارش، آگاهی از حسابرسی و حضور الکترونیکی و همچنین توانمندسازی کارکنان (تان، گود، و ریچاردسون[8] ۲۰۲۰). در نهایت، مطالعات دیگر اثر بازدارنده تحریم‌ها و آموزش را بر رفتار فیشینگ بررسی کرده‌اند. مجازات‌های رفتار انحرافی از اقدامات اصلاحی خفیف، مانند درخواست از کارکنان برای انجام آموزش، تا اتهامات جنایی یا مدنی متغیر است (آیگفو و همکاران، ۲۰۲۰، ۱۱۶۰).

تحقیقات رفتار سازمانی نشان می دهد که تفاوت های فردی در عملکرد شغلی کارکنان، یادگیری سازمانی (آموزش) و موفقیت شغلی نقش دارند (فانگ[9] و همکاران ۲۰۱۵، ۱۲۴۰). آجزن [10](۲۰۱۱، ۱۱۵) پیشنهاد می کند که برای بهبود درک ما از رفتار انسانی، عادت، رفتار گذشته، و عوامل پس زمینه، مانند ویژگی های شخصیتی، باید در نظریه رفتار برنامه ریزی شده گنجانده شوند. در این

1 Michen
2 Gratian
3 Burns
4 Furnell
5 Chen
6 Meta-analysis
7 Trang
8 Tan
9 Fang et al
10 Ajzen

راستا، مطالعات امنیت اطلاعات تأثیر عادت و ویژگی‌های شخصیتی را بر رفتار و قصد رفتاری افراد مورد بررسی قرار داده‌اند. عادت‌ها به عنوان دنباله‌های آموخته‌شده از اعمالی تعریف می‌شوند که به پاسخ‌های خودکار به نشانه‌های خاص تبدیل شده‌اند و برای دستیابی به اهداف معین ضروری هستند . مطالعات قبلی امنیت اطلاعات در مورد نقش عادت نشان داده است که واریانس توضیح داده شده در مدل نظری با گنجاندن عادت افزایش می‌یابد (سامستاد و همکاران[1]، ۲۰۱۹ ،۳۴۸). ونس[2] و همکاران (۲۰۱۸ ،۳۶۰) نشان می دهد که قرار گرفتن در معرض هشدارهای مکرر منجر به کاهش پایبندی به هشدارهای امنیتی می شود. این نشان می‌دهد که رفتار معمولی یک کارمند ممکن است بدون فرآیند شناختی زیاد ادامه یابد، و در شرایط دشوار و زمانی که انگیزه‌ها به جای دیگری هدایت شوند، ظاهر می‌شود. این یافته های گذشته نشان می دهد که عادت به طور بالقوه می تواند بر قصد رفتاری امنیتی فرد تأثیر بگذارد.

منش و ویژگی های شخصیتی یک فرد معمولاً بر قصد رفتاری امنیتی آنها تأثیر می گذارد(جوهانسون[3] و همکاران،۲۰۱۶ ،۲۴۰). گراتیان و همکاران (۲۰۱۸ ،۳۵۲) دریافتند که تفاوت‌های فردی و ویژگی‌های شخصیتی تفاوت‌ها در قصد رفتار امنیت سایبری افراد را نشان می‌دهد. به طور مشابه، جانستون[4] و همکاران (۲۰۱۶ ،۲۴۰) گزارش می دهد که افراد به موقعیت های مشابه در زمینه امنیت اطلاعات واکنش متفاوتی نشان می دهند. این مطالعات ارتباط بین ویژگی های شخصیتی کارکنان و قصد رفتار امنیتی آنها را نشان می دهد. در روانشناسی، محققان مشاهده کرده اند که افراد خاصی که رویدادهای بسیار استرس زا را تجربه می کنند، اما انعطاف پذیر و سالم باقی می مانند، دارای یک ویژگی شخصیتی متفاوت به نام سرسرختی[5] هستند. سرسختی به طور گسترده در روانشناسی، تحقیقات نظامی و مدیریت سازمانی مورد مطالعه قرار گرفته است (کاوو و گارسیا[6]،۲۰۱۸ ،۳۶۸). سر سختی به معنای توانایی ارزیابی عوامل استرس‌زا، مواجهه عمدی با این عوامل و شجاعانه عمل کردن است. این یک الگوی فکری و عملی است که عوامل استرس‌زا را از یک بلا و فاجعه احتمالی به یک فرصت برای رشد تبدیل می‌کند. به عنوان مثال، در یک مطالعه طولی ۱۲ ساله که در یک شرکت مخابراتی انجام شد، کارمندانی که سطوح بالایی از سرسختی داشتند، علیرغم تحولات استرس زا که شرکت تجربه کرد، بهتر از همکاران خود در سلامت و عملکرد پیشرفت کردند. بارتون[7] و همکاران (۲۰۱۲ ،؟؟) دریافتند که مصرف بیش از حد الکل و سوء مصرف در افسران نظامی با سطوح پایین سرسختی به دلیل ناتوانی آنها در مقابله با استرسی که در محل کار با آن مواجه می شوند، شایع است. در مثالی دیگر، کالوو و گارسیا (۲۰۱۸) سرسختی را در یک رابطه تعدیل‌کننده بین توانمندسازی ساختاری و روانی مدل‌سازی کردند و دریافتند که سرسختی تأثیر فرسودگی شغلی را کاهش می‌دهد.

آموزش و پرورش به عنوان یکی از بزرگترین نهاد های آموزشی کشور نقش تعیین کننده ای در افزایش سطح آگاهی جامعه و جلوگیری از بروز خطرات نوپدید از جمله حملات سایبری دارد. مدرسه به عنوان خانه دوم دانش آموزان نقش تعیین کننده

1 Sommestad
2 Vance
3 Johnston
4 Johnston
5 Stubbornness
6 Calvo and García
7 Bartone

ای در رشد آنان و آموزش چگونگی برخود با تهدیدهای بیشمار محیطی دارد. و تمامی ارکان مدرسه برای رشد دانش آموزان و رساندن آنان به سطح بالایی از دانش و آگاهی مسئول هستند. در این پژوهش به صورت خاص توجه بر معلمان تربیت بدنی است که از حیث محبوبیت در بین دانش آموزان اهمیت ویژه ای دارند. معلمان تربیت بدنی به مانند سایر معلمان با طیف وسیعی از دانش آموزان سروکار دارند و اندیشه و تفکر آنان قابل انتقال به دانش اموزان بوده و در بسیاری از مواقع معلمان الگوهای رفتاری برای دانش آموزان محسوب می شوند. برخورد با مسائل روز دنیا و پاسخ درست و به موقع از سویی معلمان تربیت بدنی باعث انتقال درست رفتارهای صحیح و مثبت به دانش آموزان می شود؛ مسائل امنیت سایبری با توجه به رشد روز افزون ابزارهای الکترونیکی فضای مجازی و رشد شبکه های مجازی به یکی از مهترین مسائل در حوزه آموزش تبدیل شده و لزوم همکاری و واکنش های مطلوب از سویی معلمان و در این پژوهش معلمان تربیت بدنی را می طلبد. از این رو توجه به این مقوله و حوزه های روانشناختی فردی و تاثیراتی که این ویژگی ها بر جذب و یا دفع تاثیرات فضای مجازی بر جای می گذارند از مهترین شاخه های تحقیقی در عصر حدید است و در این پژوهش نیز به دلیل اهمیت این موضوع به دنبال پاسخ به این سوال هستیم که آیا سرسختی می تواند در ارتباط بین عادت با رفتارهای امنیتی سایبری نقش میانجی ایفا کند؟

روش شناسی

پژوهش حاضر کاربردی و از نوع همبستگی است که به شکل میدانی صورت گرفته است. جامعه آماری پژوهش شامل معلمان تربیت بدنی استان خراسان جنوبی به تعداد ۲۶۷ نفر در سال تحصیلی ۱۴۰۲-۱۴۰۱ بودند نمونه با توجه به جدول مورگان به تعداد ۱۵۲ نفر انتخاب شدند که شیوه نمونه گیری به صورت تصادفی ساده استفاده شد. پژوهش در بازه ۴ ماهه انجام گرفت. ابزار پژوهش شامل پرسشنامه استاندارد عادت سیپونه[1] و همکاران (۲۰۱۲) با ۶ گویه، پرسشنامه استاندارد سرسختی بارتون[2] (۲۰۰۰) با ۹ گویه و پرسشنامه قصد رفتارهای امنیت سایبری تامپسون[3] و همکاران (۲۰۱۷) با ۴ گویه مورد استفاده قرار گرفتند. پرسشنامه های تحقیق به دو صورت حضوری و پرسشنامه الکترونیکی در شبکه های مجازی در اختیار جامعه هدف قرار گرفت. برای اطمینان از روایی پرسشنامه‌ها، بعد از تدوین آن‌ها از نظرات و راهنمایی‌های ۱۰ تن از استادان صاحب‌نظر در علم مدیریت ورزش استفاده شد و نظرات آن‌ها در پرسش‌نامه نهایی لحاظ گردید. برای اطمینان از پایایی پرسشنامه‌ها ۳۰ نسخه آن در مطالعه مقدماتی بر روی نمونه که به‌طور کاملاً تصادفی از تمام شهرهای استان خراسان جنوبی انتخاب‌شده بود، توزیع شد و بعد از جمع آوری تمامی پرسشنامه توزیع شده، ضریب آلفای کرونباخ برای پرسشنامه های عادت (α=۰/۸۹)، سرسختی (α=۰/۸۴) ، و برای قصد رفتارهای امنیت سایبری (α=۰/۷۹) بدست آمد. در ادامه برای تجزیه‌و تحلیل داده‌ها از روش‌های آمار توصیفی (میانگین، انحراف معیار) و استنباطی (کالموگروف-اسمیرنوف،مدل سازی معادلات ساختاری) با استفاده از نرم افزارهای اس.پی.اس.اس. نسخه ۲۲ و اسمارت پلاس نسخه ۳ در سطح معناداری p≤ ۰۵ استفاده شد.

1
2
3

یافته ها

ارائه یافته‌های تحقیق در دو بخش توصیفی و استنباطی صورت گرفت که در قسمت بیان نتایج توصیفی داده‌ها، در باب یافته‌های جمعیت شناختی، نتایج به شرح جدول ۱ بود.

جدول ۱. یافته های جمعیت شناختی

	متغیر	فراوانی	درصد فراوانی
جنسیت	مرد	۷۰	۴۶/۰۵
	زن	۸۲	۵۳/۹۴
تحصیلات	کاردانی	۱۰	۶/۵۷
	کارشناسی	۹۸	۶۴/۴۷
	کارشناسی ارشد و دکتری	۴۴	۲۸/۹۴
سابقه	زیر ۱۰ سال	۲۶	۱۷/۱۰
	۱۱ تا ۲۰ سال	۶۹	۴۵/۳۹
	۲۱ تا ۳۰ سال	۵۷	۳۷/۵

در این پژوهش به منظور بررسی مدل مفهومی تحقیق از روش معادلات ساختاری با نرم افزار **PLS** استفاده شد که نتایج حاصل از این اندازه گیری به شرح ذیل می باشد.

برای بررسی پایایی متغیرهای تحقیق از دو شاخص پایایی ترکیبی و آلفای کرونباخ استفاده شده است. پایایی ترکیبی و آلفای کرونباخ بنا به گفته فورنر و لارکر [1](۱۹۸۱) بایستی ۰/۷ یا بالاتر باشد که نشان از کافی بودن همگرایی درونی دارد. سازگاری درونی همان پایایی ست که هم از الفای کرونباخ استفاده می‌شود و هم از پایایی ترکیبی. هر دو شاخص به بررسی سازگاری درونی می پردازند. برای تمامی متغیرهای تحقیق مقدار آلفای کرونباخ و پایایی ترکیبی از ۰/۷ بزرگتر شده اند که نشان از پایایی ابزار اندازه گیری می‌باشد.

جدول ۲. معیارهای آلفای کرونباخ، پایایی ترکیبی و روایی همگرای متغیرهای پژوهش

متغیرهای مکنون	ضریب آلفای کرونباخ (Alpha ≥ 0/7)	ضریب پایایی ترکیبی (CR ≥ 0/7)	میانگین واریانس استخراج شده (AVE ≥ 0/5)
سرسختی	۰/۷۱	۰/۷۹	۰/۵۲
عادت	۰/۷۰	۰/۷۲	۰/۶۱
قصد رفتار امنیت سایبری	۰/۷۲	۰/۷۶	۰/۵۱

1 Fornell and Larcker

همان‌گونه که در جدول ۲، نشان داده شده است، هر سه متغیر پنهان پژوهش دارای مقدار آلفای کرونباخ و پایایی ترکیبی بالای ۰/۷ می‌باشند و مناسب بودن وضعیت پایایی را می‌توان مورد قبول دانست.

جهت بررسی روایی واگرای مدل اندازه‌گیری از معیار فورنل و لارکر استفاده شد. بر اساس این معیارها، روایی واگرای قابل قبول یک مدل حاکی از آن است که یک سازه در مدل نسبت به سازه‌های دیگر تعامل بیشتری با شاخص‌هایش دارد. طبق این شاخص واریانس هر متغیر مکنون باید برای شاخص‌های مربوط به خودش بیشتر از سایر شاخص‌ها باشد.

جدول ۳. ماتریس همبستگی و (آزمون فورنل لاکر)AVE

متغیرهای مکنون	سرسختی	عادت	قصد رفتار امنیت سایبری
سرسختی	۰/۵۵		
عادت	۰/۸۴	۰/۵۶	
قصد رفتار امنیت سایبری	۰./۸۷	۰/۸۶	۰/۶۶

همان‌گونه که در جدول ۳، مشاهده می‌شود، روایی واگرای مدل در حد مناسبی بوده است.

جدول ٤. ضریب تعیین متغیر درونزای و شاخص برازش مدل

متغیرهای درونزا	سرسختی	قصد رفتار امنیت سایبری
ضریب تعیین	۰/۷۱	۰/۸۱

بر اساس نتایج در جدول ۴، ضریب تعیین برای متغیر درونزا مقدار قابل قبول است که کیفیت مدل ساختاری را نشان می‌دهد.

جدول ۵. برآورد پارامترهای مدل ساختاری

متغیر	شاخص اشتراکی	شاخص افزونگی (Q^2)
سرسختی	۰/۱۶	۰/۱۹
عادت	۰/۱۵	–
قصد رفتار امنیت سایبری	۰/۱۱	۰/۳۳

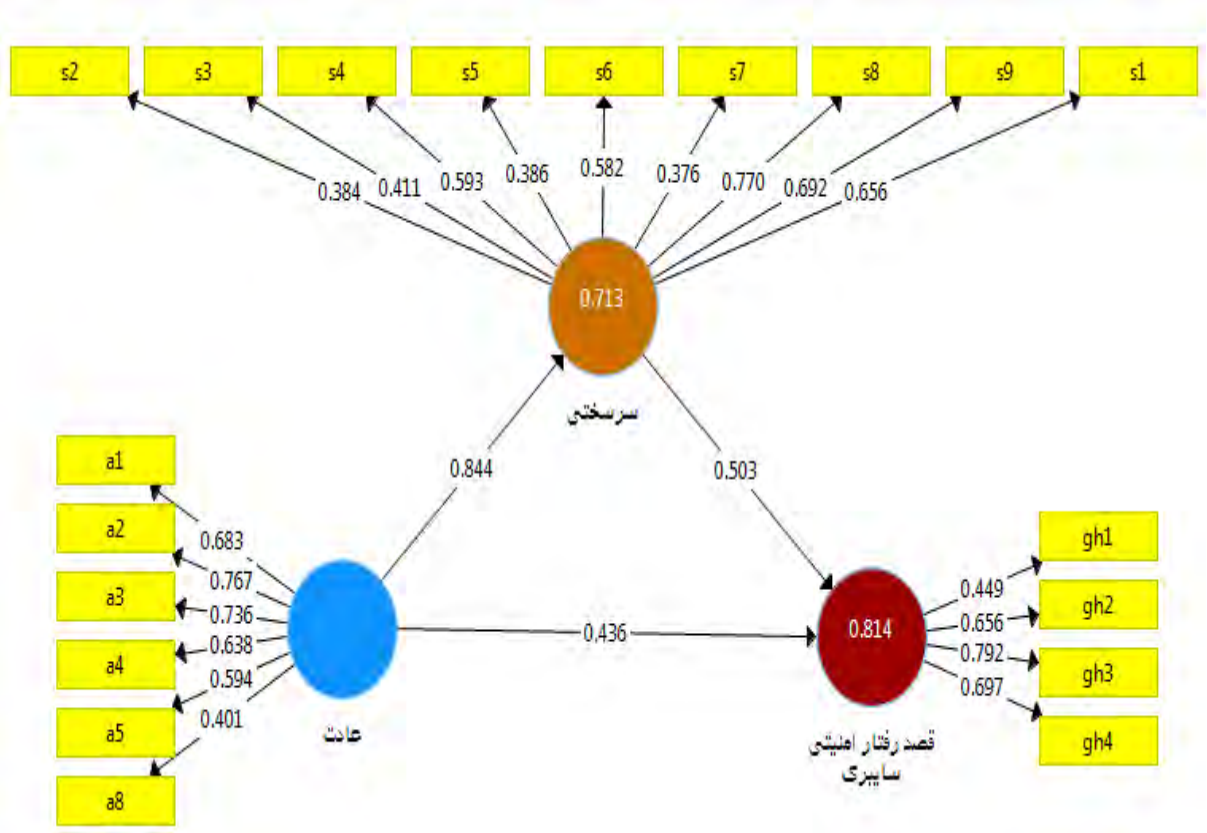
با توجه به جدول ۵، شاخص افزونگی فقط برای متغیرها درونزا (متغیر ملاک) محاسبه می‌گردد و مانند شاخص اشتراکی باید مقدار آن مثبت باشد. در کتاب‌های آماری سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ را به عنوان مقادیر ضعیف، متوسط و قوی برای GOF معرفی نموده‌اند. لذا با توجه به نتایج مقدار این دو شاخص نیز مطلوب گزارش می شود.

$$GOF = \sqrt{\overline{Communalities} * R^2} = \sqrt{0.54 * 0.76} = 0.64$$

جدول ٦. ضرایب مسیر مدل ساختاری و اثر کل متغیرها

مسیر	ضریب اثر استاندارد	t-value	سطح معناداری
عادت به سرسختی	۰/۸۴	۷۷/۱۵	۰/۰۰۱
عادت به قصد رفتار امنیت سایبری	۰/۴۳	۸/۱۲	۰/۰۰۱
سرسختی به قصد رفتار امنیت سایبری	۰/۵۰	۹/۴۸	۰/۰۰۱
عادت > سرسختی > قصد رفتار امنیت سایبری		۹/۶۸	۰/۰۰۱

همانطور که از جدول ۶، استنباط می‌شود کلیه مسیر های بین متغیرها تحقیق معنی دار است.

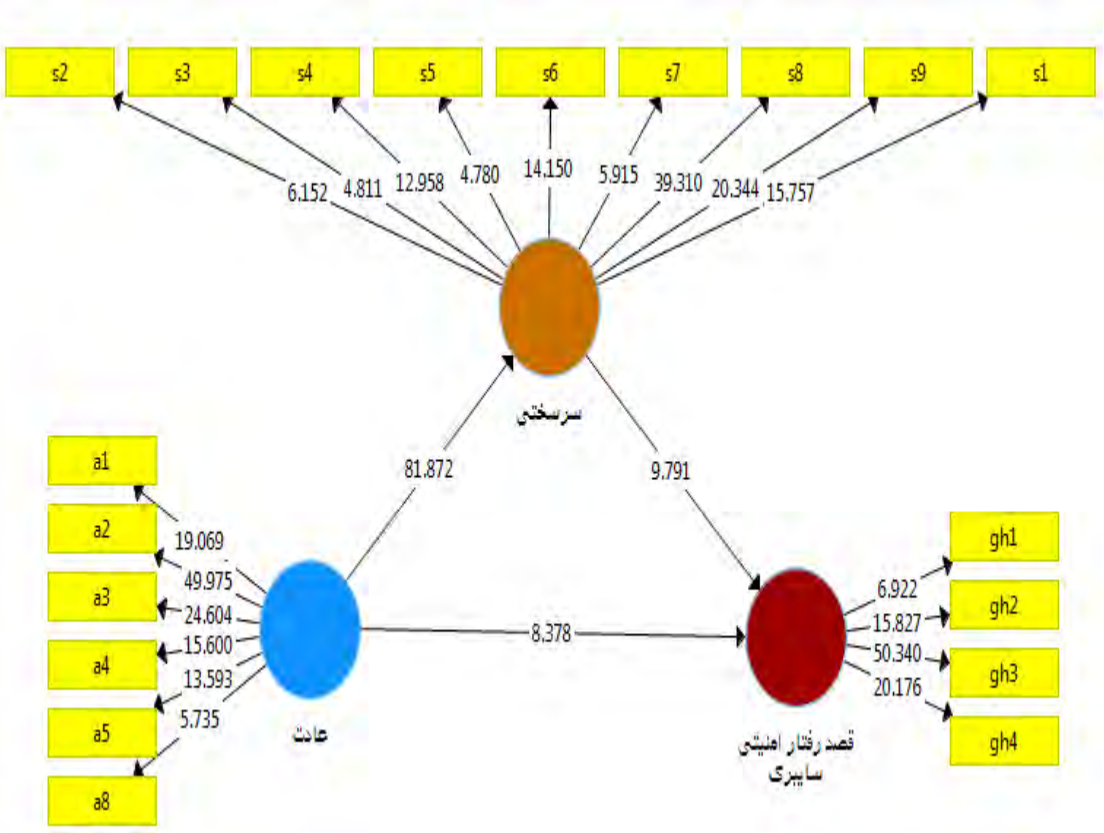


شکل ۱. مدل در حالت تخمین ضرایب استاندارد

شکل ۱ مدل تحلیل عاملی تاییدی و معادلات ساختاری را در حالت تخمین ضرایب استاندارد نشان می‌دهد. در این نمودار اعداد و یا ضرایب به دو دسته تقسیم می‌شوند. دسته‌ی اول تحت عنوان معادلات اندازه گیری هستند که روابط بین متغیرهای پنهان (متغیرهای اصلی تحقیق) و آشکار (سوالات پرسشنامه) می‌باشد (روابط بین بیضی و مستطیل)، این معادلات را اصطلاحاً بارهای عاملی[1] گویند. دسته‌ی دوم معادلات

1 Loading factor

ساختاری هستند که روابط بین متغیرهای پنهان و پنهان می‌باشند به این ضرایب اصطلاحاً ضرایب مسیر[1] گفته می‌شود و برای آزمون فرضیات استفاده می‌شوند.



شکل ۲. مدل پژوهش در حالت ضرایب تی

مدل ۲ در واقع تمامی معادلات اندازه گیری (بارهای عاملی) و معادلات ساختاری (ضرایب مسیر) را با استفاده از آماره t، آزمون می کند. بر طبق این مدل، بار عاملی در سطح اطمینان ۹۵٪ معنادار می‌باشد اگر مقدار آماره‌ی t خارج بازه ۱/۹۶- تا ۱/۹۶+ قرار گیرد.

می توان نقش میانجیگری سرسختی را به کمک آزمون سوبل[2] نیز آزمون کرد. آماره آزمون سوبل به صورت زیر محاسبه می شود :

a: مقدار ضریب مسیر میان متغیر مستقل و میانجی

b: مقدار ضریب مسیر میان متغیر میانجی و وابسته

sa: خطای استاندارد مربوط به مسیر میان متغیر مستقل و میانجی

sb: خطای استاندارد مربوط به مسیر میان متغیر میانجی و وابسته

1 Path coefficient
2 Sobel test

$$\mathbf{z-value} = \frac{\boldsymbol{a \times b}}{\sqrt{(\boldsymbol{b^2 \times S_a^2}) + (\boldsymbol{a^2 \times S_b^2}) + (\boldsymbol{S_a^2 \times S_b^2})}} =$$

مقدار آماره سوبل برای سرسختی ۳/۵۸ گزارش شد که چون از مقدار بحرانی ۱/۹۶ بیشتر است می توان گفت که سرسختی در ارتباط بین عادت با رفتار امنیتی سایبری نقش میانجی دارند.

بحث و نتیجه گیری

هدف از پژوهش حاضر نقش میانجی سرسختی در ارتباط عادت با قصد رفتار امنیتی سایبری در معلمان تربیت بدنی خراسان جنوبی بود. نتایج تحقیق نشان داد، سرسختی بر قصد انجام رفتارهای امنیتی سایبری تاثیر گذار است. نتایج تحقیقات گذشته تأیید می‌کند که ویژگی‌های شخصیتی به‌عنوان ویژگی‌های درونی می‌تواند بر قصد رفتار کارکنان برای رعایت امنیت تأثیر بگذارد. گراتین و همکاران (۲۰۱۸) در پژوهشی ارتباطاتی را بین ویژگی‌های شخصیتی کارکنان و قصد رفتار پیدا کرده‌اند(گراتین[1] و همکاران،۲۰۱۸). مطالعه حاضر شواهد بیشتری از وجود این ارتباط ارائه می دهد. در زمینه امنیت اطلاعات، نتایج نشان می‌دهد که ویژگی‌های شخصیتی سرسختی نقش کلیدی در تعیین نگرش و قصد رفتار امنیتی کارکنان دارد. این بدان معناست که معلمان تربیت بدنی که سطوح بالایی از سرسختی (تعهد، کنترل و چالش) دارند، می‌توانند در صورت لزوم تنظیماتی را برای به حداقل رساندن تأثیر تهدیدات امنیتی انجام دهند تا اینکه خود را از آن دور کنند یا در برابر تهدید امنیتی تسلیم شوند. معلمان تربیت بدنی با محیطی سروکار دارند که چالش و هیجان یکی از ویژگی های اصلی آن است و این خاصیت محیطی ورزش می تواند در ایجاد رفتارهای امنتیتی نقش تعیین کننده ای ایفا کند. ادبیات نشان می دهد که سطوح بالای سرسختی به احتمال زیاد کارکنان را قادر می سازد تا با شرایط دشوار کنار بیایند. مطالعه ما نشان می‌دهد که معلمان تربیت بدنی ممکن است بر اساس سطوح سرسختی خود به سیاست‌ها، رویه‌ها و تهدیدات امنیتی متفاوت پاسخ دهند و تلاش‌های امنیتی انطباقی را برانگیزند، مشروط بر اینکه دارای سطوح بالایی از همه سرسختی باشند. تمایل به تعهد سرسختی ممکن است انگیزه رفتار کارکنان را برای مشارکت در (توسعه شاخص های امنیتی مثبت) ایجاد کند، زیرا تعهد مستلزم ارتباط عمیق با سازمان بدون توجه به پیچیدگی‌های کار است. معلمانی که به شدت به سازمان خود متعهد هستند، بر حفاظت از دارایی های اطلاعاتی تمرکز می کنند و به امنیت اطلاعات علاقه دارند تا به جای منافع خودشان به نفع سازمان باشند (پوسی، رابرتز و لوری ۲۰۱۵، ۲۵). مطالعات گذشته در مورد سرسختی نشان داده است که تعهد در تقویت تاب آوری در افراد مفید است. این بدان معناست که کارکنانی که سطح بالایی از تعهد را نشان می دهند همچنین نشان می دهند که ممکن است سازگارتر باشند و احتمالاً منابع امنیتی را از محیط کار خود برای محافظت از دارایی های اطلاعات سازمانی به کار گیرند. تمایل به کنترل سرسختی نیز مهم است، زیرا کارکنان با سطح کنترل بالا بسیار خوش بین هستند که می توانند بر روی رویدادهای کاری اطراف خود تأثیر بگذارند تا نتایج مطلوب حاصل شود. که این ممکن است به عنوان یک مکانیسم انگیزشی درونی در معلمان عمل کند و آنها را قادر می‌سازد تا از دانش امنیتی، مهارت‌ها، توانایی‌ها و تخصص خود برای برآورده کردن خواسته‌های سیاست‌های امنیتی در محل کار استفاده

1 Gratian

کنند. این جنبه با پوسی و همکاران (۲۰۱۵) مطابقت دارد که نشان می‌دهد کارمندانی که در توانایی‌های خود احساس توانایی و شایستگی بالایی می‌کنند، احتمالاً از سیاست‌های امنیتی پیروی می‌کنند و با تهدیدات امنیتی مقابله می‌کنند.

نتایج تحقیق نشان داد، عادت به طور قابل توجهی بر قصد رفتار امنیتی معلمان تربیت بدنی تأثیر می گذارد. این یافته با هوواو و همکاران (۲۰۱۶)در مورد نقشی که عادت بر قصد کارمندان برای پیروی از سیاست های امنیتی ایفا می کند، همسو است. علاوه بر این، اگر کارمندان سیاست های امنیتی را به عنوان محدودیت آزادی شخصی درک کنند(هوواو و پاتری[1]، ۲۰۱۶، ۴۰)؛ در غیاب عادات امنیتی قوی، چنین کارکنانی ممکن است از رویه های امنیتی در محل کار پیروی نکنند. علاوه بر این، پاسخ‌های خودکار مانند عادت‌ها ممکن است زمانی که کارکنان موقعیت‌های استرس‌زا را تجربه می‌کنند، شایع‌تر باشند. کارمندان ممکن است از نظر شناختی تحت تأثیر الزامات امنیتی در محل کار قرار گیرند و باعث می شود آنها اقدامات یا رفتارهایی را انجام دهند که ناشی از یک فکر یا فرآیند تصمیم گیری خودکار است. به عنوان مثال، معلمانی که با استرس محل کار سر و کار دارند ممکن است به طور معمول یک وظیفه کاری را انجام دهند و توجه کمتری به اطلاعات جدیدی داشته باشند که ممکن است نشان دهنده وجود تهدیدات امنیتی باشد. به همین ترتیب، کارمندانی که احساس می کنند محل کارشان امن است ممکن است کمتر از تهدیدات امنیتی در محیط آگاه باشند، بنابراین به آنها اجازه می دهند تا به طور خودکار پاسخ دهند. این یافته‌ها نشان می‌دهد که وقتی توانایی‌های شناختی کارکنان کاهش می‌یابد، احتمالاً پاسخ‌های عادتی ممکن است بر قصد رفتار امنیتی آنها تأثیر بگذارد. این نتیجه ادبیات عادت را در متن امنیت اطلاعات گسترش می دهد و تأثیر قوی عادت را بر قصد رفتار امنیتی کارکنان برجسته می کند.

یافته‌های این تحقیق ادبیات فعلی در مورد عادت در زمینه‌های امنیت اطلاعات را گسترش می‌دهد. نتایج نشان می‌دهد که اگر کارمندان از نظر شناختی بیش از حد تحت فشار باشند، چه منفی (استرس کاری) و چه مثبت (آرام)، پاسخ‌های معمولی ممکن است بر قصد رفتار امنیتی آنها تأثیر بگذارد. درک تأثیر عادات کارکنان به عنوان رفتار گذشته و پاسخ های خودکار با توجه به قصد رفتار امنیتی آنها مهم است. تا زمانی که یک محرک ثابت بماند، قصد رفتار ممکن است تغییر نکند (آجزن،۲۰۰۲ ۱۱۰). هنگامی که عادت کردن به یک محرک آشنا شروع می شود، ممکن است به سایر محرک های جدید تعمیم داده شود، به خصوص اگر آنها ویژگی های مشابهی داشته باشند (اندرسون و همکاران،۲۰۱۷، ۴۵). نتایج نشان می‌دهد که پاسخ‌های خودکار کارکنان اغلب با نشانه‌های خاص ممکن است به طور قابل‌توجهی بر قصد رفتار امنیتی تأثیر بگذارد. این پژوهش، چندین پیامد برای متخصصان و سازمان‌های امنیت اطلاعات دارد. نتایج نقش مهم ویژگی‌های شخصیتی سرسختی را در توسعه رفتار امنیتی کارکنان نشان می‌دهد. مطالعات قبلی کارکنان را با استفاده از پنج ویژگی شخصیتی بزرگ طبقه‌بندی کرده‌اند و مدیریت پیام‌های متقاعدکننده را بر اساس ویژگی‌های شخصیتی کارکنان پیشنهاد کرده‌اند (جانستون و همکاران ۲۰۱۶، ۲۴۱). با این حال، نتایج ما نشان می‌دهد که مدیریت باید از طریق مداخلات هدفمند برای توسعه تعهد، کنترل و گرایش‌های چالشی کارکنان، ویژگی‌های سرسختی شخصیتی را در کارکنان ایجاد کند. کارکنان با ویژگی‌های سرسختی قوی، راهبردهای مقابله‌ای را توسعه می‌دهند و مشکل‌گشا هستند.

1 Hovav and Putri

معلمان تربیت بدنی نیروهای تاثیر گذار بر دانش آموزان هستند و اقدامات و رفتارهای انها می توان اثرات مثبت و منفی فراوانی برای آموزش و پرورش ایجاد کند و مدیران نباید از این عملکرد مهم معلمان تربیت بدنی غافل باشند و باید همواره رفتارها آنان به ویژه در جهت اقدامات سایبری که پدیده نو است، همواره مورد توجه باشد. با توجه به نتایج تحقیق پشنهاد می شود، مقوله امنیت سایبری و حملات سایبری در مدارس کشور به طور جد مورد اموزش قرار گیرد و معلمان بخشی از اموزش خود را با توجه به اهمیت فضای مجازی به این موضوع اختصاص دهند. در این پژوهش به طور خاص معلمان تربیت بدنی مورد بررسی قرار گرفتند و تاثیر گذاری انان بر دانش اموزان را با درک مفاهیم امنیت سایبری و انتقال ان به دانش اموزان را از طریق معلمان تربیت بدنی از مهمترین اهداف این تحقیق بود. تعامل بیشتر آموزش و پرورش با نیروهای انتظامی و استفاده از خبرگان در این نهادها برای انتقال دانش خود از فضای مجازی و سایبری به دانش آموزان نیز یکی دیگر از راهکارهای آشنایی بیشتر دانش آموزان با فضای سایبری و خطرات این حوزه است.

هر پژوهشی در مسیر اجرایی خود با یکسری از محدودیت هایی برخورد می کند که تا حدودی در سرعت انجام آن اختلال ایجاد می کند از جمله محدودیت های این پژوهش عدم همکاری برخی از معلمان در تکمیل کردند پرسشنامه پژوهش و درخواست های مکرر برای انجام این مهم بود و از جمله محدودیت های مهم دیگر مفهوم و موضوع امنیت سایبری بود که به دلیل اینکه یکی از مهمترین موضوعات روز است در مدارس و سطح آموزش و پرورش خیلی کم به آن پرداخته شده بود و نبود تحقیقات در این حوزه باعث ضعیف بودن مقوله ی پیشینه تحقیق شده بود.

Reference

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology, 41(6), 1151-1170.

Ajzen, I. 2002. “Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives.”Personality and Social Psychology Review 6: 107–122. doi:10.1207/S15327957PSPR0602_02.

Anderson, B. B., A. Vance, J. L. Jenkins, C. B. Kirwan, and D. Bjornn. 2017. “It All Blurs Together: How the Effects ofHabituation Generalize Across System Notifications and Security Warnings.” In Information Systems andNeuroscience, edited by F. D. Davis, R. Riedl, J. vom Brocke, P.-M. Léger, and A. B. Randolph, 43–49. Cham: Springer International Publishing. doi:10.1007/978-3-319-41402-7_6

Bartone, P. T. 2012. “Social and Organizational Influences on Psychological Hardiness: How Leaders Can Increase Stress Resilience.” Security Informatics 1: 21. doi:10.1186/2190- 8532-1-21.

Beloredi, T,. Tayari, M (2023). Government measures to create cyber security, 1(4): 64-76.

Burns, A. J., C. Posey, J. F. Courtney, T. L. Roberts, and P. Nanayakkara. 2017. “Organizational Information Securityas a Complex Adaptive System: Insights from Three Agent-Based Models.” Information Systems Frontiers 19: 509–524. doi:10.1007/s10796-015-9608-8.

Calvo, J.-C. A., and G. M. García. 2018. “Hardiness as Moderator of the Relationship Between Structural and Psychological Empowerment on Burnout in Middle Managers.” Journal of Occupational and Organizational Psychology 91: 362–384. doi:10.1111/joop.12194

Cisco. 2018. Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today’s Threats, CYBERSECURITY SPECIAL REPORT. San Jose, CA: Cisco Systems

Chen, X., D. Wu, L. Chen, and J. K. L. Teng. 2018. “Sanction Severity and Employees’ Information Security Policy Compliance: Investigating Mediating, Moderating, and Control Variables.” Information & Management 55: 1049–1060. doi:10.1016/j.im.2018.05.011

Fang, R., B. Landis, Z. Zhang, M. H. Anderson, J. D. Shaw, and M. Kilduff. 2015. “Integrating Personality and Social Networks: A Meta-Analysis of Personality, Network Position, and Work Outcomes in Organizations.” Organization Science 26: 1243–1260. doi:10.1287/orsc. 2015.0972.

Flowerday, S. V., and T. Tuyikeze. 2016. “Information Security Policy Development and Implementation: The What, How and Who.” Computers & Security 61: 169– 183. doi:10.1016/j.cose.2016.06.002

Furnell, S., W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li. 2018. “Enhancing Security Behaviour by Supporting the User.” Computers & Security 75: 1–9. doi:10.1016/j.cose. 2018.01.016.

Gratian, M., S. Bandi, M. Cukier, J. Dykstra, and A. Ginther. 2018. “Correlating Human Traits and Cyber Security Behavior Intentions.” Computers & Security 73: 345–358. doi:10.1016/j.cose.2017.11.015

Herath, T., M.-S. Yim, J. D’Arcy, K. Nam, and H. R. Rao. 2018. “Examining Employee Security Violations: MoralDisengagement and its Environmental Influences.” Information Technology & People. doi:10.1108/ITP-10- 2017-0322.

Hovav, A., and F. F. Putri. 2016. “This is My Device! Why Should I Follow Your Rules? Employees’ Compliancewith BYOD Security Policy. Pervasive and Mobile Computing, Mobile Security.” Privacy and Forensics 32: 35–49. doi:10.1016/j.pmcj.2016.06.007.

Johnston, A. C., M. Warkentin, M. McBride, and L. Carter. 2016. “Dispositional and Situational Factors: Influences on Information Security Policy Violations.” European Journal of Information Systems 25: 231–251. doi:10.1057/ ejis.2015.15

Posey, C., T. L. Roberts, and P. B. Lowry. 2015. “The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets.” Journal of Management Information Systems 32: 179–214. doi:10. 1080/07421222.2015.1138374

Safa, N. S., C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh, and M. Sookhak. 2019. “Deterrence and Prevention-Based Model to Mitigate Information Security Insider Threats in Organisations.” Future Generation Computer Systems 97: 587–597. doi:10.1016/j.future.2019.

Sommestad, T., H. Karlzén, and J. Hallberg. 2019. “The Theory of Planned Behavior and Information Security Policy Compliance.” Journal of Computer Information Systems 59: 344–353. doi:10.1080/08874417.2017.1368421

Tan, M. K. S., S. Goode, and A. Richardson. 2020 “Understanding Negotiated Anti-Malware Interruptio Effects on User Decision Quality in Endpoint Security.” Behaviour & Information Technology, 1–30. doi:10.1080/0144929X.2020.1734087

Trang, S. 2018. “When Does Deterrence Work? A Moderation Meta-Analysis of Employees’ Information Security Policy Behavior.” In Thirty Ninth International Conference oInformationSystems,SanFrancisco2018,17.SanFrancisco,CA.

Vance, A., J. L. Jenkins, B. B. Anderson, D. K. Bjornn, and C. B. Kirwan. 2018. “Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments.” MIS Quarterly 42: 355–380. doi:10.25300/MISQ/2018/14124

Verizon. 2019.Data Breach Investigations Report (12th), Data Breach Investigations Report. USA: Verizon.