Research Paper

Analyzing the Factor Structure of the Scale "Evaluation of Cyber Security Culture and Awareness" (Case study: Employees of Bank branches in Ahvaz City)

Sedigheh Heydari[1], Majid Barzegar[2*], Amir Hossein Mohammad Davoudi[3]

1- Ph.D. Student in Assessment and Measurement, Department of Psychology, Islamic Azad University, Saveh Branch, Saveh, Iran.

2- Assistant Professor, Department of Psychology, Islamic Azad University Marvdasht Branch, Marvdasht, Iran.

3- Associate Professor, Department of Educational Management, Faculty of Humanities, Islamic Azad University, Saveh Branch, Saveh, Iran.

Received: 2022/09/27
Revised: 2022/11/21
Accepted: 2023/01/13

Use your device to scan and read the article online

DOI:
10.30495/JPMM.2023.31055.3716

Keywords:
Factor structure, Reliability, Culture and Awareness, Cyber Security.

Abstract

Introduction & Objective: This research was conducted with the aim of analyzing the factor structure of the scale "evaluation of cyber security culture and awareness" among the Employees of bank branches Ahvaz city in the spring and summer of 2022.

Method: The research method was based on psychometric methods (factor analysis) and the tool used was the researcher-made scale for the evaluation of cyber security culture and awareness (2022). The population of employees of bank branches Ahvaz city and the statistical sample is 581 employees who were selected by simple random method. The method of data analysis was factor structure, EFA and CFA, and Cronbach's alpha coefficient.

Discussion: The fundings showed that the Cronbach's alpha coefficient was 0.88 in reliability and factor structure obtained during the EFA had favorable fit indices (CFI, GFI, RFI, NFI, IFI) covering 6 factors (inefficient human resources, budgeting and awareness, capacity building, employee position, culture of protection of information and security behavior and understanding).

Conclusion: The results showed that this scale has an acceptable factor structure and reliability among bank employees; Therefore, this tool can be used as a reliable tool to evaluate and rank the factors affecting the promotion of cyber security culture and awareness among the employees of Bank of Country branches.

Citation: Heydari S, Barzegar M, Mohammad Davoudi AH. Analyzing the Factor Structure of the Scale "Evaluation of Cyber Security Culture and Awareness" (Case study: Employees of Bank branches in Ahvaz City): Journal of Psychological Methods and Models 2023; 14 (51): 113-126.

***Corresponding Author:** Majid Barzegar
Address: Assistant Professor, Department of Educational Psychology, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran.
Tell: 09173111060
Email: mbarzegar55@gmail.com

Extended Abstract

Introduction

Today's world is highly dependent on electronic technology and protecting this data from cyber-attacks is a challenging issue. For this purpose, different organizations use different solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information about the latest information technology data, and so far, various methods have been proposed by researchers around the world to prevent cyber-attacks or reduce their damage [1]. Studies have shown that efforts are aimed at increasing awareness and culture in the cyber domain because awareness and culture regarding cyber security provide a critical factor that may help improve successful cyber security policies or guidelines in organizations [2].

In general, the lack of knowledge and experience, work processes, prioritization of behavior and environmental suitability are among the factors that affect the level of culture and awareness of a person regarding cyber security. In this regard, things like weak computer and user account security; Unsafe use of e-mail; Using USB and personal devices; remote access and work at home; lack of encryption, backup, updating and poor physical security [37], training [7, 15, 22, 34]; Specialist forces [38]; Personnel participation [7]; trust [14, 23, 26, 28, 32, 39, 40, 41]; competence [3, 4, 11, 26]; Evaluation [3, 4, 8, 10, 13, 15, 22]; Threat response ability [9, 15, 26, 40] and commitment [2, 8, 14, 20, 22, 40, 42] play a role in cybersecurity culture and awareness. Given that increasing cyber security is an ongoing challenge for security professionals and research consistently shows that online users are a weak link in cybersecurity, and in particular, privacy behavior and attitudes are influenced by culture compared to other variables. psychological and demographic (such as gender and computer expertise); Also, what kind of data people share is derived from their culture, and in fact, culture affects these choices, and in fact, certain personality traits affect user cyber security-related behavior in different cultures; Therefore, providing a tool to help solve the challenges faced by security professionals in the field of education and awareness related to cyber security in the form of culture building is necessary. Therefore, this research was conducted with the aim of analyzing the factor structure of the scale "evaluation of cyber security culture and awareness" among the Employees of bank branches Ahvaz city in the spring and summer of 2022.

Materials and Methods

The research method was based on psychometric methods (factor analysis) and the tool used was the researcher-made scale for the evaluation of cybersecurity culture and awareness (2022). This scale has a self-report form, which is set in the form of 41-items, and finally, after examining its factorial structure in the present study, 6 valid subscales were created as inefficient human resources (8 items), budgeting and awareness (8 items), capacity building. (7 items), employee position (3 items), information protection culture (5 items) and security behavior and understanding (3 items) are covered and all are scored on a 7-point Likert scale to evaluate the level of cyber security culture and awareness. Items are rated on a 7-point scale from "strongly disagree" to "strongly agree". In this scale, 14-items were reverse scored, 7-items were removed in the survey and the final structure had 34 items, therefore the total score of the scale can be between 34 and 238 and a higher score indicates a higher level of culture and awareness of the individual. Cyber security is in sub-scales and total scale. Content validity of this tool for a total of 41-items produced through literature review; It was independently reviewed and confirmed by 11 experts.

The population of employees of bank branches Ahvaz city and the statistical sample is 581 employees who were selected by simple random method. The method of

data analysis was factor structure, EFA and CFA, and Cronbach's alpha coefficient.

Findings

In the first EFA, without fixing the factors; A number of 9-factors were identified that obtained an initial eigenvalue higher than 1; But two factors covered only one topic, so they were removed from the total of factors. In the next step, out of the 7-investigated factors, one factor was removed from the total of factors due to having an unacceptable Cronbach's alpha value (0.536) and 6-final factors remained, which together explained and preserved 50.96% of the total variance. Fitness indexes, except GFI and NFI, other indexes have shown favorable values. If at least 3-fit indices are within the acceptable range, and on the other hand, three important indices of relative chi-square (x2/df), root mean square error of approximation (RMSEA) and square root of the difference between the residuals of the standardized sample covariance matrix (SRMR) are within the standard range, the fit of the model can be confirmed. Therefore, the 6-factor model discovered as a result of exploratory factor analysis is confirmed in the first-order confirmatory factor analysis. The fundings showed that the Cronbach's alpha coefficient was 0.88 in reliability.

Discussion

Factor structure obtained during the EFA had favorable fit indices (CFI, GFI, RFI, NFI, IFI) covering 6 factors (inefficient human resources, budgeting and awareness, capacity building, employee position, culture of protection of information and security behavior and understanding).

Results

The results showed that this scale has an acceptable factor structure and reliability among bank employees; therefore, this tool can be used as a reliable tool to evaluate and rank the factors affecting the promotion of cyber security culture and awareness among the employees of Bank of Country branches.

Ethical Considerations and Compliance with ethical guidelines

The participants took part in the study with full consent.

Funding

Part of the costs of this research was funded by the Applied Research Office of the Isfahan Police Force.

Authors' contributions

All authors contributed equally to the article.

Conflicts of Interest

The authors declared no conflict of interest.

مقاله پژوهشی

تحلیل ساختار عاملی مقیاس" ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری" (مطالعه موردی: کارمندان شعب بانک در شهر اهواز)**

صدیقه حیدری[۱]، مجید برزگر[۲]*، امیرحسین محمّدداودی[۳]

۱- دانشجوی دکترای سنجش و اندازه گیری، گروه روان‌شناسی، دانشکده روان‌شناسی، دانشگاه آزاد اسلامی، واحد ساوه، ساوه، ایران.

۲- استادیار گروه روان شناسی، دانشگاه آزاد اسلامی واحد مرودشت، مرودشت، ایران.

۳- دانشیار گروه مدیریت آموزشی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی، واحد ساوه، ساوه، ایران.

**- این مقاله برگرفته از رساله دکتری نویسنده اول بوده که تحت حمایت سازمانی دفتر تحقیقات کاربردی فرماندهی انتظامی استان اصفهان انجام شده است.

تاریخ دریافت: ۱۴۰۱/۰۷/۰۵
تاریخ داوری: ۱۴۰۱/۰۸/۳۰
تاریخ پذیرش:۱۴۰۱/۱۰/۲۳

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید

DOI:
10.30495/JPMM.2023.31055.3716

واژه‌های کلیدی:
ساختار عاملی، اعتبار، فرهنگ و آگاهی، امنیت سایبری.

چکیده

مقدمه و هدف: این پژوهش با هدف تحلیل ساختار عاملی مقیاس "ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری" در بین کارمندان بانک شهر اهواز در بهار و تابستان سال ۱۴۰۱ انجام شد.

روش: روش پژوهش با تکیه بر روش‌های روانسنجی (تحلیل عاملی) و ابزار مورد استفاده مقیاس محقق ساخته ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری (۱۴۰۱) بوده است. جامعه کارمندان شعب بانک شهر اهواز و نمونه آماری ۵۸۱ نفر کارمند بوده که به شیوه تصادفی ساده انتخاب شدند. روش تجزیه و تحلیل داده‌ها در بررسی ساختار عاملی، تحلیل عاملی اکتشافی و تحلیل عاملی تاییدی و در بررسی اعتبار، ضریب آلفای کرونباخ بوده است.

بحث: یافته‌ها نشان داد ضریب آلفای کرونباخ به مقدار ۰/۸۸ حاصل شده و ساختار عاملی بدست آمده طی تحلیل اکتشافی از شاخص‌های برازندگی (CFI، GFI، RFI، NFI، IFI) مطلوبی برخوردار بوده است که پوشش دهنده ۶ عامل (منابع انسانی ناکارآمد، بودجه‌بندی و آگاه‌سازی، ظرفیت‌سازی، موقعیت کارمند، فرهنگ حفاظت از اطلاعات و رفتار و درک امنیتی) می‌باشد.

نتیجه‌گیری: نتایج نشان داد این مقیاس در بین کارمندان بانک دارای ساختار عاملی و اعتبار قابل قبولی است؛ از این رو، می‌توان این ابزار را به عنوان ابزاری معتبر جهت ارزیابی و رتبه‌بندی عوامل موثر بر ارتقاء فرهنگ و آگاهی امنیتِ سایبری در بین کارمندان شعب بانک کشور بکار برد.

* **نویسنده مسئول:** مجید برزگر
نشانی: استادیار گروه روان شناسی، دانشگاه آزاد اسلامی واحد مرودشت، مرودشت، ایران..
تلفن: ۰۹۱۷۳۱۱۱۰۶۰
پست الکترونیکی: mbarzegar55@gmail.com

مقدمه

دنیای امروز به شدت به فناوری الکترونیکی وابسته است و محافظت از این داده‌ها در برابر حملات سایبری یک مسئله چالش برانگیز است. برای این منظور، سازمان‌های گوناگون از راه حل‌های گوناگون برای جلوگیری از آسیب‌های ناشی از حملات سایبری استفاده می‌کنند. امنیت سایبری، اطلاعات لحظه‌ای را در مورد آخرین داده‌های فناوری اطلاعات دنبال می‌کند و تاکنون، روش‌های گوناگونی توسط پژوهشگران در سراسر جهان برای جلوگیری از حملات سایبری یا کاهش آسیب‌های ناشی از آن‌ها پیشنهاد شده است [۱].

مطالعات نشان داده است که تلاش‌ها در جهت افزایش آگاهی و فرهنگ‌سازی در حوزه سایبر است چرا که آگاهی و فرهنگ در خصوص امنیت سایبری عامل حیاتی را ارائه می‌دهد که ممکن است به بهبود سیاست‌ها یا راهکارهای امنیت سایبری موفق در سازمان‌ها، کمک کند [۲].

پژوهش‌های بسیاری برای فرهنگ و آگاهی امنیت سایبری دو بُعد سازمانی [۳، ۴، ۵، ۶، ۷، ۸، ۹، ۱۰] و فردی [۵، ۱۱] را همراه با آگاهی، به عنوان ابعاد فرهنگ و آگاهی امنیت سایبری گزارش کرده‌اند.

کولینز و هیندز (۲۰۲۱) انگیزش درونی و بیرونی و تأثیرات اجتماعی و سازمانی را از جمله عوامل موثر بر فرهنگ و آگاهی امنیت سایبری گزارش نموده [۱۲] و جورجیادو و همکاران در پژوهشی [۵] فرهنگ سازمانی و فردی و در پژوهش دیگری [۱۱] عواملی همچون استرس عاطفی، عوامل امنیتی مرتبط با انسان، رفتار امنیتی، نگرش و شایستگی کارکنان، هیجانات، افکار و باورها، درک خطر امنیتی، آگاهی امنیتی، سابقه شغلی، تهدید خودی، نارضایتی، رویدادهای استرس‌زا و استعدادهای شخصیتی، تجربه کاری و تخصص تهدیدات سایبری مرتبط با انسان را از جمله عوامل موثر بر فرهنگ فردی گزارش نموده‌اند [۱۱].

حسن و همکاران (۲۰۲۱) [۱۳] در پژوهشی چارچوب "فناوری-سازمان-محیط زیست" را بمنظور بررسی مجموعه‌ای جامع از عوامل موثر بر آمادگی یا آگاهی امنیت سایبری سازمان ها و تأثیرات این عوامل بر عملکرد سازمان (مالی و غیرمالی) با واسطه بهبود عملکرد امنیت سازمانی، تهیه کردند. نتایج نشان داد آگاهی امنیت سایبری بر عملکرد امنیت سازمانی تأثیر مطلوب داشته که به نوبه خود بر عملکرد مالی و غیرمالی اثر مثبت می گذارد. چارچوب ارائه شده، می‌تواند برای هدایت پژوهش‌های آینده و افزایش درک فعلی از چگونگی تجهیز بهتر سازمان‌ها برای کمینه کردن وقوع و تأثیر حملات سایبری مورد استفاده قرار گیرد.

جورجیادو و همکاران (۲۰۲۱ پ) در پژوهشی به منظور طرح یک ابزار با هدف ارزیابی فرهنگ امنیت سایبری زیرساخت‌های حیاتی در بحران کووید-۱۹ (زمانی که واقعیت زندگی و شرایط کار به طور اساسی تحت تأثیر قرار گرفت) ارائه داده‌اند. ریشه این ابزار در چارچوب فرهنگ امنیتی است که در دو سطح سازمانی و فردی طبقه‌بندی شده است، سپس در ۱۰ بعد گوناگون امنیتی شامل ۵۲ حوزه تجزیه و تحلیل شده است [۴].

پاپاتساروچا و همکاران (۲۰۲۱) [۱۴] با مطالعه متون حوزه امنیت سایبری بیان کردند مجرمان سایبری این روزها بیش‌تر انسان‌ها را هدف قرار می‌دهند، زیرا سعی می‌کنند با سوءاستفاده از نقاط ضعف کاربران، اهداف مخرب خود را به انجام برسانند. بنابراین، آسیب‌پذیری‌های انسانی تهدیدی جدی برای امنیت و یکپارچگی سیستم‌ها و داده‌های رایانه‌ای است. گرایش بشر به اعتماد و کمک به دیگران و هم‌چنین، خصوصیات شخصی، اجتماعی و فرهنگی، نشان دهنده مقدار حساسیت است که ممکن است شخص نسبت به انواع خاصی از حملات و استراتژی‌های فریب‌کاری از خود نشان دهد. نتایج حاصل از بررسی متون نشان داد ارزیابی آسیب‌پذیری انسان در چارچوب‌های گوناگونی با هدف ارزیابی ظرفیت امنیت سایبری سازمان‌ها گنجانده شده است، اما این امر به ارزیابی یک بار و نه به صورت مداوم، مربوط می‌شود. افزون بر این، بدخواهی انسان هنوز در چارچوب‌های فعلیِ ارزیابیِ آسیب‌پذیری انسان نادیده گرفته می‌شود.

در بررسی متون موجود در حوزه فرهنگ و آگاهی امنیت سایبری، مواردی همچون بودجه‌بندی و جلوگیری از نفوذ هکرها [۱۵]، برنامه‌ریزی زیرساخت‌های فنی [۱۰، ۱۶، ۱۷، ۱۸، ۱۹]، ظرفیت‌سازی (اقدامات مبتنی بر وجود برنامه‌های پژوهش و توسعه) [۲۰]، برنامه‌های آموزشی [۸، ۱۱، ۲۱]، کار تیمی [۱۱]، مدیریت برنامه‌های امنیتی و مدیریت امنیت کاربر [۲۲]، پشتیبانی [۱۹]، روش‌های جدید به اشتراک‌گذاری اطلاعات، کار گروهی، اجرای سیاست‌های امنیتی و رویکردهای جدید در آموزش [۱۰] به عنوان مواردی اثرگذار در فرهنگ و آگاهی امنیت سایبری گزارش شده‌اند.

بر اساس بررسی‌های انجام شده از متون موجود، مواردی همچون عوامل فردی (ویژگی‌های شخصیتی)، عوامل خانوادگی (جامعه‌پذیری ناقص، فرسایش سرمایه اجتماعی-خانوادگی)، عوامل اجتماعی (فرسایش سرمایه اجتماعی، بسته بودن حوزه عمومی، تغییرات سبک زندگی، ناکامی‌های اجتماعی، مدیریت نامناسب اوقات فراغت، اعتراض اجتماعی)، عوامل فرهنگی (فرسایش اعتقادات و باورهای دینی، فقر فرهنگی)، عوامل اقتصادی (تنگناهای اقتصادی، احساس محرومیت نسبی، رواج فساد در جامعه)، عوامل سیاسی و قضایی (فقدان قوانین به روز و

کارآمد، غلبه تفکر سختگیرانه در دستگاه قضایی، نبود برنامه‌ریزی و سیاست‌گذاری در زمینه فضای مجازی، فقدان شفافیت در ساختار و عملکرد حاکمیت و دولت)، جذاب نبودن برنامه‌های داخلی، نبود فضای مناسب برای تخلیه احساسات و هیجانات [۲۳]؛ سطح پایین آگاهی، مشکلات روحی–روانی، اشکالات ساختار فنی فضای مجازی [۲۴]؛ افشاگری [۲۵]؛ ناآگاهی، پایین بودن فرهنگ استفاده از فضای مجازی، نارضایتی کارکنان از فشار کاری، عدم تناسب نیروی انسانی با کار، استفاده از گوشی هوشمند و رعایت نکردن ملاحظات امنیتی در محل کار، ضعف دانش کارکنان، آشنا نبودن به مباحث روز فناوری‌های نوین [۲۶]؛ منابع انسانی ناکارآمد [۲۷]، مهندسی اجتماعی [۲۱، ۲۸، ۲۹، ۳۰، ۳۱، ۳۲، ۳۳، ۳۴، ۳۵] و عدم آمادگی [۳۶] در فرهنگ و آگاهی امنیت سایبری اثرگذارند.

به طور کلی فقدان آگاهی و تجربه، فرآیندهای کاری، اولویت بندی رفتار و تناسب محیطی از جمله عواملی بوده که بر سطح فرهنگ و آگاهی فرد نسبت به امنیت سایبری اثرگذارند. در این راستا مواردی مانند امنیت ضعیف رایانه و حساب کاربری؛ استفاده ناامن از ایمیل؛ استفاده از USB و دستگاه‌های شخصی؛ دسترسی از راه دور و کار در منزل؛ عدم رمزگذاری، پشتیبان‌گیری، به‌روزرسانی و امنیت فیزیکی ضعیف [۳۷]، آموزش [۷، ۱۵، ۲۲، ۳۴]؛ نیروهای متخصص [۳۸]؛ مشارکت پرسنل [۷]؛ اعتماد [۱۴، ۲۳، ۲۶، ۲۸، ۳۲، ۳۹، ۴۰، ۴۱]؛ شایستگی [۳، ۴، ۱۱، ۲۶]؛ ارزیابی [۳، ۴، ۸، ۱۰، ۱۳، ۱۵، ۲۲]؛ توانایی پاسخگویی به تهدید [۹، ۱۵، ۲۶، ۴۰] و تعهد [۲، ۸، ۱۴، ۲۰، ۲۲، ۴۰، ۴۲] در فرهنگ و آگاهی امنیت سایبری نقش دارند.

با توجه به اینکه افزایش امنیت سایبری یک چالش مداوم برای متخصصان امنیتی است و پژوهش‌ها به گونه مداوم نشان می‌دهد که کاربران آنلاین یک حلقه ضعیف در امنیت سایبری هستند و به طور ویژه، رفتار و نگرش به حریم خصوصی تحت تأثیر فرهنگ در مقایسه با سایر متغیرهای روان‌شناختی و جمعیتی (مانند جنسیت و تخصص رایانه) قرار می‌گیرد؛ هم‌چنین، اینکه مردم چه نوع داده‌هایی را به اشتراک می‌گذارند، برگرفته از فرهنگ آنان بوده و در واقع، فرهنگ بر این انتخاب‌ها تأثیر می‌گذارد و در حقیقت ویژگی‌های شخصیتی خاصی بر رفتار مرتبط با امنیت سایبری کاربر در فرهنگ‌های گوناگون تأثیر می‌گذارد؛ بنابرین، ارائه ابزاری به منظور کمک به رفع چالش‌های پیش روی متخصصان امنیتی در حوزه آموزش و آگاهی بخشی مرتبط با امنیت سایبری در قالب فرهنگ‌سازی، ضروری به نظر آمده است.

با توجه به مطالب ذکر شده، ارائه ابزاری معتبر جهت اندازه‌گیری این متغیر در کشور احساس شد. بنابراین، تصمیم بر آن شد تا پژوهشی با هدف بررسی مقدماتی ساختار "ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری" انجام می‌شود تا به پاسخ این سوال دست یابیم که ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری دارای چگونه ساختاری است؟

روش

این پژوهش از نوع پژوهش‌های کمّی بوده و از لحاظ هدف کاربردی، از لحاظ روش با تکیه بر روش‌های روانسنجی (تحلیل عاملی) و از نظر روش جمع‌آوری کتابخانه‌ای و میدانی است. جامعه آماری این پژوهش عبارت است از کلیه کارمندان شعب بانک شهر اهواز که در سال ۱۴۰۱ مشغول به کار می‌باشند.

در این پژوهش به دلیل اینکه قصد بر بررسی روایی سازه و اعتبار یک ابزار محقق ساخته است و در واقع در تلاش ارائه یک ابزار جدید و معتبر در کشور (ایران) هستیم، این‌رو شایسته است حجم نمونه بالایی در نظر گرفته شود بنابراین، مطابق با نظر کلاین (۲۰۰۴) در هنگام استفاده از تحلیل عاملی اکتشافی و تحلیل عاملی تاییدی، برای هر متغیر مشاهده‌پذیر ۱۰ تا ۲۰ نمونه لازم است. از این‌رو حجم نمونه را در هر سطح به ازای هر گویه ۱۰ نفر با احتساب ریزش نمونه برآورد نموده که مشتمل بر ۸۴۱ نفر کارمند بود که به شیوه تصادفی ساده انتخاب شدند. با توجه به اینکه انجام تحلیل عاملی اکتشافی و تاییدی نباید بر روی یک نمونه صورت بگیرد؛ از این رو، قلمرو زمانی اجرای پژوهش در سه بازه زمانی خردادماه (برای مرحله آزمایشی)، تیرماه (برای سطح تحلیل عاملی اکتشافی) و مردادماه (برای سطح تحلیل عاملی تاییدی) به ترتیب با تعداد ۵۰، ۴۵۱ و ۳۴۰ نمونه در نظر گرفته شد. جهت جمع‌آوری داده‌ها نیز از مقیاس محقق ساخته با عنوان "ارزیابی فرهنگ و آگاهی امنیت سایبری" (۱۴۰۱) استفاده شد.

ابزار پژوهش

مقیاس محقق ساخته "ارزیابی فرهنگ و آگاهی امنیت سایبری" (۱۴۰۱):

این مقیاس دارای یک فرم خودگزارش بوده که در قالب ۴۱ گویه تنظیم شده و در نهایت، پس از بررسی ساختار عاملی آن در این پژوهش، ۶ زیرمقیاس معتبر را با عنوان منابع انسانی ناکارآمد (۸ گویه)، بودجه‌بندی و آگاه‌سازی (۸ گویه)، ظرفیت‌سازی (۷ گویه)، موقعیت کارمند (۳ گویه)، فرهنگ حفاظت از اطلاعات (۵ گویه) و رفتار و درک امنیتی (۳ گویه) پوشش داده و همگی در یک طیف ۷ درجه‌ای لیکرت برای ارزیابی سطح فرهنگ و آگاهی امنیت سایبری، نمره‌گذاری می‌شوند. گویه‌ها در طیف ۷ درجه‌ای از "کاملاً مخالفم" تا "کاملاً موافقم" رتبه‌بندی می‌شوند. در این مقیاس ۱۴ گویه نمره‌گذاری معکوس را داشته، ۷ گویه در بررسی

انجام شده حذف و ساختار نهایی دارای ۳۴ گویه بوده است، از این‌رو نمره کل مقیاس می‌تواند بین ۳۴ تا ۲۳۸ باشد و نمره بالاتر نشان دهنده سطح بالاتر فرهنگ و آگاهی فرد نسبت به امنیت سایبری در زیرمقیاس‌ها و مقیاس کل است.

روایی محتوی این ابزار برای مجموع ۴۱ گویه تولید شده از راه بررسی متون؛ به طور مستقل توسط ۱۱ متخصص بررسی و تایید شد. ۳۴ مورد از این گویه‌ها برای تحلیل عامل اکتشافی حفظ شدند.

بمنظور بررسی روایی سازه نیز در این پژوهش از تحلیل عامل اکتشافی و تاییدی بهره گرفته شد که یافته‌های آن در بخش یافته‌ها گزارش شده است. بررسی اعتبار ابزار نیز با استفاده از ضریب آلفای کرونباخ برآورد شده‌است.

یافته‌ها

از مجموع ۸۴۱ نسخه توزیع شده تعداد ۶۷۱ نسخه دریافت (نرخ بازگشت ۷۹/۷۹ درصد) و پس از حذف داده‌های پرت، تعداد ۵۰ داده برای مرحله آزمایشی (بررسی اعتبار اولیه) و تعداد ۵۸۱ داده برای هر دو سطح تحلیل (۳۷۹ داده برای تحلیل عاملی اکتشافی و ۲۰۲ داده برای تحلیل عاملی تاییدی) مورد استفاده قرار گرفت (نرخ نسخه‌های سالم ۹۴/۰۴ درصد). یافته‌های حاصل از بررسی ویژگی‌های جمعیت شناختی نشان داد، میانگین سنی افراد نمونه بین ۳۴ تا حدود ۳۷ سال با سابقه اشتغال بین ۸ تا حدود ۱۱ سال بوده است. کمترین سن ۲۳ سال، بیش‌ترین سن ۵۲ سال، کم‌ترین سابقه اشتغال ۱ و بیش‌ترین سابقه اشتغال ۲۵ سال بوده است. در خصوص جنسیت نیز، جنسیت مرد، بیش‌ترین فراوانی را به خود اختصاص داده بوده‌اند.

بررسی اعتبار اولیه ابزار با استفاده از ضریب آلفای کرونباخ

با توجه به اینکه شرط روایی، اعتبار می‌باشد؛ از این رو ابتدا اقدام به بررسی اعتبار در سطح نمونه آزمایشی گردید. یافته‌های حاصل از بررسی ضریب آلفای کرونباخ حاکی از آن بود که مقدار این ضریب بالاتر از ۰/۷ بوده و تک تک ۴۱ گویه سهم مثبتی در کل مقیاس داشته، از این رو همه ۴۱ گویه در این مرحله حفظ شدند.

بررسی روایی سازه ابزار با استفاده از تحلیل عاملی

همان‌گونه که در بخش روش پژوهش اشاره شد؛ انجام تحلیل عاملی اکتشافی و تحلیل عاملی تاییدی نباید بر روی یک نمونه و هم‌زمان باشد، از این رو جهت کشف ساختار ابزار محقق ساخته، بر داده‌هایی که از خرداد تا تیرماه جمع‌آوری شد، اقدام به انجام تحلیل عاملی اکتشافی شد و داده‌هایی که در اوایل مردادماه جمع‌آوری شده بود، به منظور انجام تحلیل عاملی تاییدی کنار گذاشته شد.

از آنجایی که انجام هر تحلیل آماری منوط به رعایت پیش‌فرض‌های آن تحلیل است؛ پیش‌فرض تحلیل عاملی اکتشافی نیز دارا بودن شاخص کفایت نمونه‌برداری (KMO) بالاتر از ۰/۷ است. مطابق جدول (۱) شاخص کفایت نمونه‌برداری بالاتر از ۰/۷ حاصل شده از این رو مجاز به انجام تحلیل اکتشافی بوده‌ایم.

جدول ۱- شاخص کفایت نمونه‌برداری

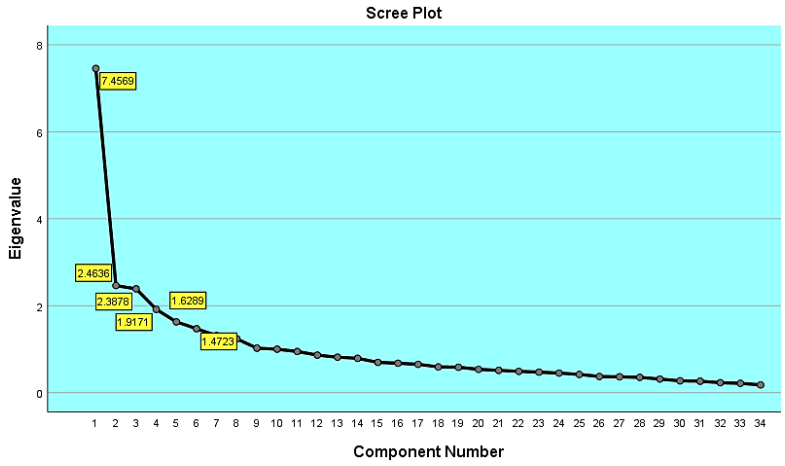
شاخص	مقدار
کایزر مایر اولکین	۰/۸۰
کرویت بارتلت/ کای اسکوئر	۴۷۴۲/۸۸
درجه آزادی	۵۶۱
سطح معناداری	۰/۰۰۱

در نخستین تحلیل عاملی اکتشافی انجام شده بدون فیکس کردن عامل‌ها؛ تعداد ۹ عامل شناسایی شد که ارزش ویژه اولیه بالاتر از ۱ را کسب کردند، اما دو عامل تنها یک گویه را پوشش دادند، از این‌رو از مجموع عوامل حذف شدند. در مرحله بعدی از ۷ عامل بررسی شده، یک عامل بدلیل دارا بودن مقدار آلفای کرونباخ غیرقابل قبول (۰/۵۳۶) از مجموع عوامل حذف شد و ۶ عامل نهایی باقی ماند که روی هم رفته ۵۰/۹۶ درصد واریانس کل را تبیین کرده و حفظ شدند.

جدول ۲- توضیح واریانس با چرخش عامل‌ها در تحلیل اکتشافی

عامل	ارزش ویژه اولیه			مجموع مربعات بارها پس از چرخش		
	جمع	درصد واریانس	درصدتجمعی	جمع	درصد واریانس	درصدتجمعی
۱	۷/۴۶	۲۱/۹۳	۲۱/۹۳	۳/۷۰	۱۰/۸۷	۱۰/۸۷
۲	۲/۴۶	۷/۲۵	۲۹/۱۸	۳/۳۸	۹/۹۴	۲۰/۸۲
۳	۲/۳۹	۷/۰۲	۳۶/۲۰	۳/۲۴	۹/۵۲	۳۰/۳۴
۴	۱/۹۲	۵/۶۴	۴۱/۸۴	۳/۰۶	۸/۹۹	۳۹/۳۳
۵	۱/۶۳	۴/۷۹	۴۶/۶۳	۲/۰۱	۵/۹۱	۴۵/۲۴
۶	۱/۴۷	۴/۳۳	۵۰/۹۶	۱/۹۴	۵/۷۲	۵۰/۹۶

بر اساس جدول (۲) پس از اعمال چرخش متعامد جهت انتخاب بهترین قرارگیری بارها، تعداد ۶ عامل ارزش ویژه بالاتر از ۱ را کسب کرده‌اند که روی هم رفته ۵۰/۹۶ درصد واریانس کل را تبیین کرده‌اند. نمودار سنگریزه (نمودار ۱) تایید کننده این یافته است.



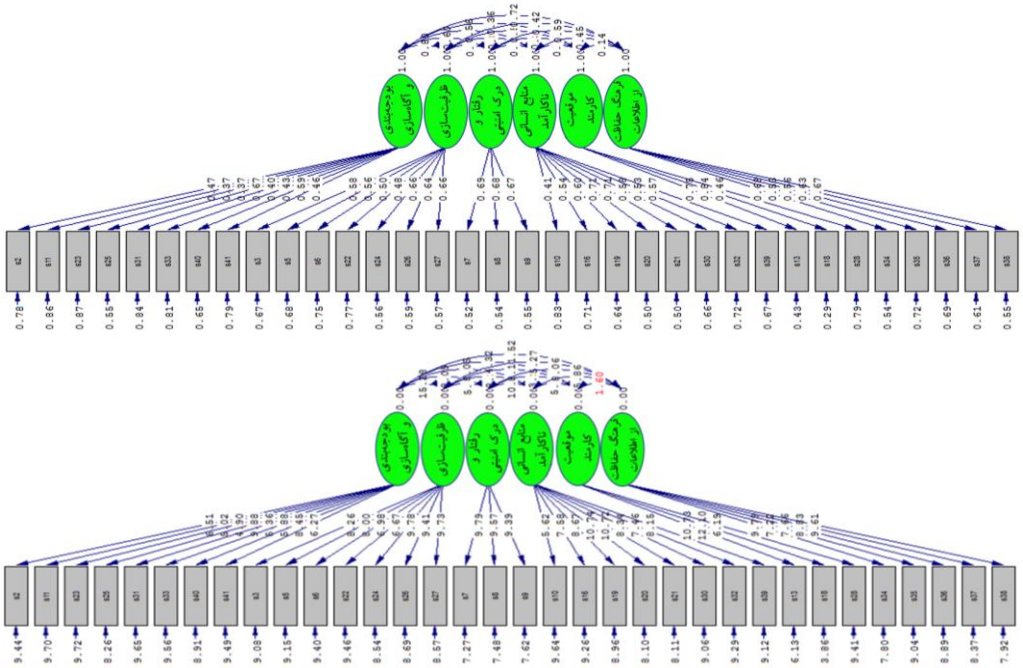
نمودار ۱- نمودار سنگریزه‌ای

جدول ۳- بارعاملی هر گویه پس از چرخش به تفکیک عامل

منابع انسانی ناکارآمد		ظرفیت‌سازی		فرهنگ حفاظت از اطلاعات		بودجه‌بندی و آگاه‌سازی		موقعیت کارمند		رفتار و درک امنیتی	
کدگویه	بار	کدگویه	بار	کدگویه	بار	کدگویه	بار	کدگویه	بار	کدگویه	بار
s20	۰/۷۶۳	s27	۰/۷۵۷	s37	۰/۷۰۱	s25	۰/۴۰۸	s18	۰/۶۸۳	s7	۰/۸۰۴
s21	۰/۷۳۹	s6	۰/۶۳۸	s36	۰/۶۸۷	s40	۰/۶۸۵	s13	۰/۶۵۶	s9	۰/۷۸۵
s30	۰/۶۳۸	s24	۰/۶۲۷	s34	۰/۶۸۵	s23	۰/۶۳۱	s28	۰/۵۲۹	s8	۰/۷۷۵
s19	۰/۶۰۰	s3	۰/۵۹۴	s35	۰/۶۴۸	s2	۰/۶۱۴				
s16	۰/۵۷۴	s22	۰/۵۵۱	s38	۰/۶۳۹	s41	۰/۴۹۰				
s32	۰/۵۷۱	s27	۰/۴۶۵			s31	۰/۴۷۸				
s39	۰/۵۱۴	s26	۰/۳۴۷			s33	۰/۴۱۹				
s10	۰/۴۶۲					s11	۰/۴۱۶				

در جدول (۳) بار عاملی به تفکیک هر عامل پس از اِعمال چرخش واریمکس و با فیکس کردن بار روی ۰/۳ محاسبه شده است به منظور تایید عوامل شناسایی شده در نتیجه انجام چرخش متعامد (واریمکس) در نرم‌افزار SPSS، در داده‌های دوم نمونه

(که در مردادماه جمع‌آوری شدند)، از نرم‌افزار Lisrel نسخه 8.80 استفاده شد.



شکل ۱- مدل ساختاری عامل‌ها بالا براساس بار استاندارد و پایین براساس مقادیر T

بر اساس شکل (۱) همان‌گونه که در مدل مشاهده می‌شود تمامی گویه‌ها نسبت به عامل مربوطه خود مقدار T بیش‌تر از ۱/۹۶ و بار استاندارد بالاتر از ۰/۳ را نشان داده و مطلوب بوده‌اند.

جدول ۴- شاخص‌های برازندگی مدل

نوع شاخص	شاخص‌ها	مقدار به‌دست آمده	مقدار قابل قبول
مطلق	کای اسکوئر هنجار شده(CMIN)	۱۰۱۴/۲۳	–
	p	۰/۰۰۱	کمتر از ۰/۵۰
	ریشه‌ی میانگین مجذورات خطای تقریب (RMSEA)	۰/۰۷۰	کمتر از ۰/۰۸
	ریشه دوم تفاوت بین پسماندهای ماتریس کواریانس نمونه استانداردشده (SRMR)	۰/۰۷۹	کمتر از ۰/۱۰
	شاخص نیکویی برازش (GFI)	۰/۸۰	حداقل ۰/۹۰
افزاینده (نسبی)	شاخص برازش مقایسه‌ای (CFI)	۰/۹۰	حداقل ۰/۹۰
	شاخص برازندگی افزایشی (IFI)	۰/۹۰	حداقل ۰/۹۰
	شاخص برازش نرم شده (NFI)	۰/۸۰	حداقل ۰/۹۰
	شاخص برازش نرم نشده (NNFI)	۰/۹۰	حداقل ۰/۹۰
صرفه‌جو(مقتصد)	کای اسکوئر نسبی (CMIN/DF)	۱/۹۸	کمتر از ۳

براساس جدول (۴) شاخص‌های برازندگی به استثناء دو شاخص GFI و NFI، سایر شاخص‌ها مقادیر مطلوبی را نشان داده‌اند. در صورتی که دست‌کم ۳ شاخص برازش در محدوده قابل قبول قرار گیرد و از سویی دیگر سه شاخصِ مهمِ کای اسکوئر نسبی (x^2/df)، ریشه میانگین مجذورات خطای تقریب (RMSEA) و ریشه دوم تفاوت بین پسماندهای ماتریس کواریانس نمونه استانداردشده (SRMR) در محدوده معیار قرار گیرند، برازش مدل قابل تایید می‌باشد. از این رو، مدل ۶ عاملی

کشف شده در نتیجه تحلیل عاملی اکتشافی، در تحلیل عاملی تاییدی مرتبه اول، مورد تایید واقع می‌شود.

بحث و نتیجه‌گیری

این پژوهش با هدف تحلیل ساختار عاملی مقیاس" ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری انجام شد. به منظور دستیابی به این هدف، با استفاده از روش‌های متداول در نظریه کلاسیک اندازه‌گیری (تحلیل عاملی اکتشافی و تاییدی) اقدام به بررسی روایی سازه ابزار شد. با توجه به اینکه شرط روایی، پایا بودن ابزار می‌باشد، ابتدا اعتبار بررسی شد و بر اساس آن تعداد ۷ گویه از مقیاس حذف شد و تحلیل عاملی اکتشافی بر ۳۴ گویه باقیمانده انجام شد. تحلیل عاملی اکتشافی نشان داد ابزار دارای ۶ عامل معتبر بوده است. این ۶ عامل حدود ۵۰ درصد از واریانس کل را تبیین کردند و ساختار آن‌ها در نتیجه تحلیل عاملی تاییدی مورد تایید واقع شد چرا که شاخص‌های برازش در محدوده قابل قبولی بدست آمدند. اعتبار هر ۶ عامل نیز با استفاده از ضریب آلفای کرونباخ بررسی شد که برای هر ۶ عامل به مقدار مطلوب و بالاتر از ۰/۷ بدست آمد.

یکی از این عوامل "بودجه‌بندی و آگاه‌سازی" بوده که مواردی همچون مدیریت بودجه‌بندی و تخصیص منابع، آموزش راه‌های جلوگیری از نفوذ هکرها، ارزیابی مهارت‌های امنیتی و شایستگی کارکنان، ناآشنایی و ناآگاهی نسبت به فناوری اطلاعات و امنیت، برنامه آگاهی از امنیت سایبری، آشنا نبودن به مباحث روز فناوری‌های نوین، آمادگی برای پذیرش فناوری‌های نوین، سواد رسانه‌ای، تعهد و مسئولیت‌پذیری را در ساختار خود جای داده است. عامل دوم "ظرفیت‌سازی" بوده که مواردی همچون فرآیندها و محیط کار (برنامه‌ریزی و کنترل کار، جریان داده‌ها و تنظیم کار)، برنامه‌ریزی زیرساخت‌های فنی، آمادگی و واکنش سایبری، رویکردهای خاص فنی، رفتاری، فرهنگی و شخصی، شناسایی خطرات امنیتی احتمالی مرتبط با انسان، داشتن تجربه کاری، اقدامات مبتنی بر وجود برنامه‌های پژوهش و توسعه، آموزش، تهدیدهای امنیت سایبری، اجرای سیاست‌های امنیتی و رویکردهای جدید در آموزش را در ساختار خود جای داده است. سومین عامل "رفتار و درک" بوده که مواردی همچون رفتار کارمندان با یکدیگر هنگام انتقال اطلاعات بانکی، درک و رفتار غیرایمن را در ساختار خود جای داده است. عامل چهارم "منابع انسانی ناکارآمد" بوده که مواردی همچون حجم کار ذهنی بالا، خستگی یا خواب آلودگی، مشکلات خانوادگی، اختلالات جدی سلامت روان، مشکلات شخصیتی، اشکالات ساختار فنی فضای مجازی، منابع انسانی ناکارآمد و اعتماد بی‌جا را در ساختار خود جای داده است. عامل دیگر "موقعیت کارمند" بوده که مواردی همچون نوع موقعیت کارمند (مقدار دسترسی، دانش، امتیازات و مهارت‌ها) و فقر فرهنگی را در ساختار خود جای داده و آخرین عامل "فرهنگ حفاظت از اطلاعات" بوده که مواردی همچون رمزگذاری سیستم محل کار، پشتیبان‌گیری، به روزرسانی، امنیت فیزیکی و وجود نیروهای متخصص را در ساختار خود جای داده است. این یافته منطبق با مبانی نظری گزارش شده در مقاله می‌باشد برای مثال، پژوهشگرانی همچون کریم‌زاده و همکاران (۲۰۲۲)، صیادی تورانلو و همکاران (۲۰۲۰)، ذاکری هامانه و همکاران (۲۰۲۰)، توکلی و همکاران (۲۰۲۱)، ایسر و برندتوینر(۲۰۲۲)، اروِلا و همکاران (۲۰۲۲)، العلوی و الباسام (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱الف، ب، پ و ت)، حسن و همکاران (۲۰۲۱)، پاپاتساروچا و همکاران (۲۰۲۱)، کولینز و هیندز (۲۰۲۱)، ممده و دبالا (۲۰۲۱) و تریم و لی (۲۰۲۱) در پژوهش‌های خود به این مولفه‌ها اشاره کرده‌اند.

با توجه به تایید ساختار این ابزار در بین کارمندان بانک، می‌توان این ابزار را به عنوان ابزاری معتبر جهت ارزیابی و رتبه‌بندی عوامل موثر بر ارتقاء فرهنگ و آگاهی امنیتِ سایبری در بین کارمندان شعب بانک کشور بکار برد. هم‌چنین، استفاده از این ابزار در گزینش کارمندان بانک، در پلیس فضای تولید اطلاعات (فتا)، بخش‌های مربوط به فراجا و جرایم سایبری و نیز قرار دادن این ابزار در کنار سایر ابزارهای مفید گزینش پیشنهاد می‌شود.

ملاحظات اخلاقی

پیروی از اصول اخلاق پژوهش

در این مطالعه فرم‌های رضایت‌نامه آگاهانه توسط تمامی شرکت‌کنندگان تکمیل شد.

حامی مالی

بخشی از هزینه‌های این پژوهش توسط دفتر تحقیقات کاربردی نیروی انتظامی استان اصفهان تامین شد.

تعارض منافع

بنابر اظهار نویسندگان این مقاله فاقد هرگونه تعارض منافع بوده است.

References

1- Yuchong L, Qinghui L. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 1-11, In Press. 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289

2- Al-Alawi AI, Al-Bassam SA. Assessing The Factors of Cybersecurity Awareness in the Banking Sector. *AGJSR* 2021, 37 (4): 17-32. https://www.researchgate.net/profile/Adel-Al-Alawi/publication/352855616

3- Georgiadou A, Mouzakitis S, Askounis D. Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems*, 2021b , 1-11. https://www.tandfonline.com/doi/abs/10.1080/08874417.2021.1903367

4- Georgiadou A, Mouzakitis S, Askounis D. Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis. *International Journal of Network Security & Its Applications (IJNSA),* 2021c, *Vol*, *13*, 33-50. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3787197

5- Georgiadou A, Mouzakitis S, Askounis D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, 2021d , *21*(9), 3267. https://www.mdpi.com/1424-8220/21/9/3267

6- Cardoso L, Castanho M. A CYBERCULTURE STUDY: K-POP AND THE NEW MEDIA-BTS AND TWITTER. *European Journal of Social Sciences Studies*, 2021, *6*(6). https://www.oapub.org/soc/index.php/EJSSS/article/view/1127/1713

7- Progoulakis I, Nikitakos N, Rohmeyer P, Bunin B, Dalaklis D, Karamperidis S. Perspectives on Cyber Security for Offshore Oil and Gas Assets. *Journal of Marine Science and Engineering*, 2021, *9*(2), 112. https://www.mdpi.com/2077-1312/9/2/112

8- Trim PR, Lee YI. The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, 2021, *5*(3), 32. https://www.mdpi.com/2504-2289/5/3/32

9- Bethel KL. *An Evaluation of Organizational Culture: Its Influence on Security Culture: A Case Study* (Doctoral dissertation, Northcentral University). 2020, https://www.proquest.com/openview/001623eb1e1a44dfce30d35f6555a6b1/1?pq-origsite=gscholar&cbl=18750&diss=y

10- Pavlova E. Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation. *Information & Security*, 2020, *46*(3), 239-249. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Enhancing+the+Organisational+Culture+related+to+Cyber+Security+during+the+University+Digital+Transformation&btnG=

11- Georgiadou A, Mouzakitis S, Askounis D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 2021a, 1-20. https://link.springer.com/article/10.1057/s41284-021-00286-2

12- Collins EI, Hinds J. Exploring workers' subjective experiences of habit formation in cyber-security: A qualitative survey. *Cyberpsychology, Behavior, and Social Networking*. 2021, Exploring workers' subjective experiences of habit formation in cyber-security: A qualitative survey — the University of Bath's research portal

13- Hasan S, Ali M, Kurnia S, Thurasamy R. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*,

2021, *58*, 102726. https://www.sciencedirect.com/science/article/abs/pii/S2214212620308656
14- Papatsaroucha D, Nikoloudakis Y, Kefaloukos I, Pallis E, Markakis E. A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues. *arXiv preprint arXiv:2106.09986*. 2021, https://arxiv.org/abs/2106.09986.
15- Sahraei M, Valavi M, Bayat B, Taraghi A. Provide a native model of cyber monitoring,monitoring and alerting based on the ooda cycle. *National Security*, 2020, 10(37), 473-512. https://ns.sndu.ac.ir/article 1118.html?lang=en
16- Erola A, Agrafiotis I, Nurse JR, Axon L, Goldsmith M, Creese S. A system to calculate cyber-value-at-risk. *Computers & Security*, 2022, *113*, 102545. Pp: 1-12.https://www.sciencedirect.com/science/article/pii/S0167404821003692
17- Ahmed OS. Teacher's awareness to develop student cyber security: A Case Study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021, *12*(10), 5148-5156. https://www.turcomat.org/index.php/turkbilmat/article/view/5297
18- Al-Ghamdi MI. Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*. 2021, https://www.sciencedirect.com/science/article/pii/S2214785321029941
19- Legárd I. Building an effective information security awareness program. *Central and Eastern European eDem and eGov Days*, 2020, *338*, 189-200. https://ejournals.facultas.at/index.php/ocgcp/article/view/1887
20- Nguyen TA, Koblandin K, Suleymanova S, Volokh V. Effects of 'Digital'Country's Information Security on Political Stability. *Journal of Cyber Security and Mobility*, 2022, 29-52. https://journals.riverpublishers.com/index.php/JCSANDM/article/view/8377
21- Matyokurehwa K, Rudhumbu N, Gombiro C, Mlambo C. Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy*, 2021, *4*(2), e141. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.141
22- Orehek Š, Petrič G. A systematic review of scales for measuring information security culture. *Information & Computer Security*. 2020, https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2019-0140/full/html
23- Karimzadeh B, Pourghahramani B, Beigi J. Designing a Native Model of Social Capital to Prevent Cybercrime. *Journal of Social Order*, 2021, *13*(2), 115-148. [in Persian] DOR:20.1001.1.20086024.1400.13.2.5.1 , http://sopra.jrl.police.ir/article 97406.html?lang=en
24- Sayyadi Tooranloo H, Mirghafoori SH, Mahdavi MR, Saghafi S. Analysis of factors related to the establishment of Cybercrime using a Fuzzy approach. *Quarterly of Order & Security Guards*, *13*(3), 27-54. 2020, [in Persian] https://doi.org/10.22034/osra.2020.94388, http://osra.jrl.police.ir/article 94388.html?lang=en
25- Razavi SY, Sadehmiri J. Influential components in raising the level of awareness and intelligence of NAJA personnel against the threats and injuries of soft war based on the intellectual system of Imam Khamenei, the Supreme Leader. *Police Protectoral and Security Studies quarterly*, 2020, *15*(55), 43-77. [in Persian] http://spaps.jrl.police.ir/article 94797.html?lang=en
26- Farashi A, Estarky A, abiri D. The role of preventive actions in protecting the organization's cyber missions. *Police*

Protectoral and Security Studies quarterly, 2020, *15*(55), 129-160. [in Persian] http://spaps.jrl.police.ir/article 94799.html?lang=en

27- Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. 2021, https://www.sciencedirect.com/science/article/pii/S0167404821000912

28- Iser B, Brandtweiner R. Role of awareness to prevent personal disasters: reducing the risks of falling for phishing by strengthening user awareness. *Wit Transactions On The Built Environment*, *207*, 79-88. 2022, https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/207/38183

29- Richardson MD, Lemoine PA, Stephens WE, Waller RE. Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, 2020, *27*(2), 23-39. Retrieved from https://eric.ed.gov/?id=EJ1252710

30- Priyadarshini I, Kumar R, Sharma R, Singh PK, Satapathy SC. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering*, *93*, 107204. 2021, https://www.sciencedirect.com/science/article/abs/pii/S0045790621002007

31- Nurse JR. Cybersecurity Awareness. *arXiv preprint arXiv:2103.00474*. 2021, https://doi.org/10.1007/978-3-642-27739-9 1596-1

32- Quayyum F, Cruzes DS, Jaccheri L. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. 2021, https://www.sciencedirect.com/science/article/pii/S2212868921000581

33- Mai PT, Tick A. Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung*, *18*, 67-89. 2021, http://acta.uni-obuda.hu/Issue115. htm

34- Khan AH, Sawhney PB, Das S, Pandey D. SartCyber Security Awareness Measurement Model (APAT). In *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)* (pp. 298-302). 2020, February, IEEE. https://ieeexplore.ieee.org/abstract/document/9087242

35- Hatzivasilis G, Ioannidis S, Smyrlis M, Spanoudakis G, Frati F, Goeke L, Koshutanski H. Modern aspects of cyber-security training and continuous adaptation of Programmes to trainees. *Applied Sciences*, 2020, *10*(16), 5702. https://www.mdpi.com/2076-3417/10/16/5702

36- Furnell S, Collins E. Cyber security: what are we talking about?. *Computer Fraud & Security*, *2021*(7), 6-11. https://www.sciencedirect.com/science/article/abs/pii/S1361372321000737

37- Coventry L, Branley-Bell D, Sillence E, Magalini S, Mari P, Magkanaraki A, Anastasopoulou K. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *International Conference on Human-Computer Interaction,* 2020, July (pp. 105-122). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-50309-3_8

38- Tavakoli F, Mortazavi M, Keshavarztork M. Determining Strategic Factors Affecting the Prevention of Cybercrime with Fuzzy Delphi Approach. *Journal of Social Order*, 2021, *12*(4), 113-140. [in Persian] DOR:20.1001.1.20086024.1399.12.4.5.8 .

http://sopra.jrl.police.ir/article 95455.html?lang=en

39- Zakeri Hamane R, Azam Azade M, GHaziNejad M, Bastani S. Qualitative

Study of Users' Sense of Online Security in Social Networks. *New Media Studies*, 2020, *6*(21), 141-178. [in Persian] https://doi.org/10.22054/nms.2020.42506.741, https://nms.atu.ac.ir/article_11875.html?lang=en

40- Uchendu B, Nurse JR, Bada M, Furnell S. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 2021, *109*, 102387. https://www.sciencedirect.com/science/article/pii/S016740482100211X

41- Mamade BK, Dabala DM. Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs. *Journal of Cyber Security and Mobility*, 699-724. 2021, https://journals.riverpublishers.com/index.php/JCSANDM/article/view/5673

42- Abebe G, Lessa L. Human Factors Influence in Information Systems Security: Towards a Conceptual Framework. *Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management Harare*. 2020, http://ieomsociety.org/harare2020/