رویش روان شناسی، سال۱۱، شماره۶، شماره پیاپی ۷۵، شهریور ۱۴۰۱
Rooyesh-e-Ravanshenasi Journal(RRJ),11(6), 2022

عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید-۱۹

Psychological Factors Affecting on the Culture and Awareness of Cyber Security in During of Covid-19 Outbreak

صدیقه حیدری
کاندیدای دکتری سنجش و اندازه گیری، دانشگاه آزاد اسلامی، واحد ساوه، ساوه، ایران.

Sedigheh Heydari
Ph.D candidate in assessment and measurement, Islamic Azad University, Saveh Branch, Saveh, Iran.
heydari_ss@yahoo.com

چکیده

پژوهش حاضر با هدف بررسی عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید-۱۹ به روش کیفی و از نوع تحلیل مضمون انجام شد. داده‌های پژوهش از اسناد بالادستی که شامل کلیه مقالات معتبر منتشر شده در سال‌های ۲۰۲۰ الی ۲۰۲۲ در داخل و خارج کشور بوده است، با ۴ کلیدواژه (فرهنگ، آگاهی، امنیت سایبری، عوامل روانشناختی) در پایگاه‌های سیویلیکا، نورمگز، مگ‌ایران، گوگل‌اسکولار، ساینس‌دایرکت جمع‌آوری و در چارچوب نرم‌افزار MAXQDA مورد بررسی قرار گرفته است. معیار ورود مقالات به پژوهش، محتوی قابل اجرا برای سوال پژوهش و مطالعات مربوط به متغیر هدف و معیارهای خروج خلاصه مقالات، فصل‌های کتاب، گزارش‌های کوتاه و عدم دسترسی به متن کامل مقاله بوده است. سنجش روایی با استفاده از روایی محتوی و برآورد پایایی داده‌ها با استفاده از روش هولستی انجام شد. یافته‌ها نشان داد از مجموع ۴۴ مضمون شناسایی شده از کدگذاری اسناد و متون بالادستی، ۶ مضمون فرعی (روانشناختی، رفتاری، خانوادگی-اجتماعی، اقتصادی، حقوقی و فنی)، تشکیل شد. براساس یافته‌ها، در بین کلیه مضمون‌های فرعی شناسایی شده، بیشترین مضمون‌ها مرتبط با مضمون روانشناختی بوده (۱۶ مضمون) که در آن مضمون‌های خودکارآمدی، دلبستگی، استرس عاطفی، هیجانات، افکار و باورها، نگرش، انگیزش، ویژگی‌های شخصیتی و سلامت روان مضامینی بودند که دارای اهمیت ویژه‌ای هستند.

واژه‌های کلیدی: *عوامل روانشـــناختی، کووید-۱۹، فرهنگ و آگاهی، امنیت سایبری، تحلیل مضمون.*

Abstract

The aim of this study was to investigate the psychological factors affecting the culture and awareness of cyber security during the period of the Covid-19 outbreak by qualitative method and theme analysis. Research data from upstream documents that include all valid articles published from 2020 to 2022 inside and outside the country, with 4 keywords (culture, awareness, cyber security, psychological factors) in the databases Civilica, Noormags, Magiran, google scholar, science direct and academia have been collected and reviewed in the framework of MAXQDA software. The criteria for entering articles in the research were the applicable content for the research question and studies related to the target variable and the criteria for excluding abstracts, book chapters, short reports, and lack of access to the full text of the article. Validity was assessed using content validity and data reliability was estimated using the Holstie method. Findings showed that out of 45 themes identified were formed from the coding of upstream documents and texts, 6 sub-themes (psychological, behavioral, family-social, economic, legal, and technical). According to the findings, among all the identified sub-themes, most themes were related to psychological themes (16 themes) in which the themes of self-efficacy, attachment, emotional stress, emotions, thoughts and beliefs, attitudes, motivation, personality traits, and health Psychics were topics of particular importance.

Keywords: *Psychological factors, Covid-19, culture & awareness, cyber security, theme analysis.*

نوع مقاله : تحلیلی **دریافت : اسفند ۱۴۰۰** **پذیرش: تیر ۱۴۰۱** **ویرایش نهایی: شهریور ۱۴۰۱**

مقدمه

با آمیخته شدن زندگی بشر با انقلاب سایبری، مبحث امنیت[1] و نوع خاص آن (امنیت سایبری[2]) مطرح می‌شود. امنیت، بنیادی‌ترین نیاز هر جامعه و مهم‌ترین عامل برای دوام زندگی اجتماعی به شمار می‌رود و از این رو از گذشته‌های دور، مورد توجه صاحب‌نظران و نظریه‌پردازان بوده است (قربان‌پور و قربان‌پور، ۱۳۹۷). مفهوم امنیت تحت تاثیر تحولات سطح کلان بین‌الملل دستخوش تغییر شده و با

1 - Security
2 -Syber Security

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

شروع روند جهانی شدن و تحت تاثیر فناوری اطلاعات و ارتباطات مفهومی چندبعدی یافته است (عابدی، ۱۳۹۸). فراگیری اینترنت و فناوری‌های جدید ارتباطی و اطلاعاتی و انقلاب ارتباطات، نوع جدیدی از ارتباطات مجازی را که خالی از روح حاکم بر روابط واقعی اجتماعی است به وجود آورده است. این امر موجب ظهور و شکل‌گیری فضای سایبری به موازات جهان واقعی شده و معادلات و الگوهای ارتباطات سنتی، تولید، انتقال و مصرف اطلاعات را به هم زده و موجب جنبش جهانی در حوزه ارتباطات و انتقال محتوا و پیام‌های ارتباطی در سریع‌ترین زمان ممکن شده است (دی‌کیمپ[1] و همکاران، ۲۰۲۰؛ اومانیلو[2] و همکاران، ۲۰۱۹). چنین فضایی که به عنوان واقعیت سایبری یکپارچه، در نظر گرفته می‌شود، برخی از مهم‌ترین محدودیت‌های دست و پا گیر موجود در دنیای فیزیکی را از میان برده و محیط جذابی برای کاربران خود به وجود آورده که باعث فریب کاربران و ایجاد اعواج در نگرش‌های آنان شده است (دی‌کیمپ و همکاران، ۲۰۲۰)، بنابراین لزوم رعایت امنیت در این فضا که امنیت سایبری نامیده می‌شود، احساس می‌گردد. حال استفاده از فضای سایبر توسط عموم مردم در چند سال اخیر به عنوان مهم‌ترین پیشران تحول دیجیتال در کشور، رشد چشمگیری داشته و با ظهور بیماری کووید-۱۹[3]، استفاده از این فضا اجتناب‌ناپذیر بوده و زندگی افراد جامعه در ابعاد مختلف آن با تسهیلات این فضا جریان دارد (گوناوان و راتمونو[4]، ۲۰۲۰)، بنابراین افزایش قدرت در فضای سایبری باعث بازدارندگی سایبری شده و منجر به افزایش امنیت سایبری کشور می‌گردد (رحیم‌اف و موحدی‌صفت، ۱۳۹۹).

کووید-۱۹ یک بیماری عفونی است که توسط ویروس سارس-کو۲[5] ایجاد می‌شود، ویروسی که عمدتاً سیستم تنفسی انسان را هدف قرار می‌دهد (روتان و بایراردی[6]، ۲۰۲۰). در ۱۱ مارس، سازمان بهداشت جهانی شیوع کووید-۱۹ را یک بیماری همه‌گیر جهانی اعلام کرد و بسیاری از کشورها به سرعت به این اعلامیه واکنش نشان دادند و با اجرای سختگیرانه محدودیت اجتماعی (که معمولاً به عنوان "قرنطینه" شناخته می‌شود) به عنوان یک اقدام موثر برای مدیریت تماس انسانی و انتقال ویروس پاسخ دادند (ما و مک‌کینون[7]، ۲۰۲۱). کووید-۱۹ به شیوه‌های مختلف بر زندگی روزمره ما تأثیر می‌گذارد و طرح‌های قرنطینه ساختارها و محیط‌های اجتماعی ما را پیکربندی و بازسازی کرده است. با دستورات ماندن در خانه، ممنوعیت سفر و قوانین فاصله‌گذاری اجتماعی، استفاده از اینترنت و همچنین وابستگی به پلتفرم‌های بر خط[8] از جمله بانکداری، مراقبت‌های بهداشتی، سرگرمی، تجارت، آموزش و خدمات ضروری دولتی، افزایش یافته است (هاکاک[9] و همکاران، ۲۰۲۰).

روال کاری بسیاری از افراد از کار در یک محیط اداری به کار در خانه (دورکاری) تبدیل شده است. برخی نیز در روند رو به رشد خرید برخط شرکت می‌کنند و افراد ممکن است به جای دیدار با دوستان یا آشنایی با افراد جدید در دنیای واقعی، در رویدادهای اجتماعی مجازی یا قرار ملاقات شرکت کنند. تغییرات در الگوهای مصرف‌کننده و واکنش‌های دولت بر اکوسیستم‌ها و اقتصادهای دنیای سایبری تأثیر گذاشته است. علی‌رغم اینکه مصرف‌کنندگان از راحتی دسترسی برخط لذت می‌برند و بسیاری از مشاغل برخط و ارائه‌دهندگان خدمات در زمینه کووید-۱۹ شکوفا شده‌اند، همه شرکت‌کنندگان برخط قانونی نیستند. به طور خاص، مجرمان سایبری اکنون فرصت‌های بیشتری برای سوءاستفاده از کاربران خدمات برخط به روش‌های خلاقانه مختلف دارند. با حرکت عمومی از فعالیت‌های حضوری به فعالیت‌های برخط، احتمال قربانی شدن جرایم سایبری نیز افزایش می‌یابد که ممکن است منجر به اختلال در خدمات، زیان مالی، نقض داده‌ها و اضطراب‌های فردی و سازمانی شود (همان منبع).

در حقیقت، ظهور کووید-۱۹ سلامت جسمی و روانی را تهدید کرده و رفتار و فرآیندهای تصمیم‌گیری افراد، سازمان‌ها و موسسات را در سراسر جهان تغییر داده است. از آنجایی که بسیاری از خدمات به دلیل شیوع همه‌گیر به صورت بر خط و دورکاری حرکت می‌کنند، کلاهبرداری سایبری[10] با موضوع کووید-۱۹ نیز در حال رشد است (ما و مک‌کینون، ۲۰۲۱) و دورکاری در شرایط قرنطینه می‌تواند تأثیراتی

1 - De Kimpe
2 - Umanailo
3 - COVID-19
4 - Gunawan & Ratmono
5 - SARS-COV2
6 - Rothan & Byrareddy
7 - Ma & McKinnon
8 - Online
9 - Hakak
10 - cyber fraud

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

بر بهزیستی و نحوه درک و تعامل مردم با فناوری برای هماهنگی، برقراری ارتباط و همکاری با دیگران داشته باشد (دئوتروم[1] و همکاران، ۲۰۲۱).

جدای از بحث در مورد دیدگاه‌های جرم‌شناسی، اعتقاد بر این است که آگاهی از زمینه روانشناختی قربانی شدن کلاهبرداری سایبری در شرایط فعلی بسیار مهم است. کووید-۱۹ نه تنها رفتار کلی افراد را تغییر داده است، بلکه تأثیر قابل توجهی بر سلامت روانی داشته است. بسیاری از افراد در طول همه‌گیری، آشفتگی‌های هیجانی را در درجات مختلفی از جمله استرس، افسردگی، تنهایی، اضطراب عمومی، بی‌خوابی و خودکشی تجربه کرده‌اند (لی[2]، ۲۰۲۰). آنچه وضعیت را بدتر می‌کند این است که به دلیل عدم حمایت اجتماعی در بسیاری از جوامع در سراسر جهان، جمعیت زیادی به دلیل از دست دادن درآمد و عدم دسترسی به لوازم اساسی زندگی از جمله غذا و سرپناه از اضطراب رنج می‌برند. این ممکن است منجر به افسردگی یا حتی آسیب رساندن به خود شود (کومار و نایار[3]، ۲۰۲۰). حال مجرمان سایبری آسیب‌پذیری‌های روانی قربانیان را هدف قرار می‌دهند و از اضطراب ناشی از کووید-۱۹ با دستکاری بی‌ثباتی‌های عاطفی برای فعال کردن کلاهبرداری سایبری استفاده می‌کنند (ما و مک‌کینون، ۲۰۲۱).

تحقیقات نایدو[4] نشان داده است که ۳۰٪ از حوادث کلاهبرداری سایبری شامل مجرمان سایبری است که قربانیان را هدف قرار می‌دهند و از آرامش به عنوان یک جذابیت احساسی استفاده می‌کنند، در حالی که ۲۲٪ از رویدادهای کلاهبرداری سایبری با ترس و ۲۲٪ دیگر با امید مرتبط هستند. دیگر جذابیت‌های احساسی مورد استفاده در کلاهبرداری سایبری عبارتند از لذت (۱۵٪)، تهدید (۶٪) و شفقت (۵٪) (نایدو، ۲۰۲۰).

از سویی دیگر، براساس گزارشی که اخیراً توسط مؤسسه پونمون[5] در ابتدای سال ۲۰۲۰ منتشر شد، فراوانی حوادث مربوط به تهدیدات داخلی از سال ۲۰۱۸ تا ۴۷ درصد افزایش یافته است و میانگین هزینه جهانی ۳۱ درصد به مبلغ ۱۱.۴۵ میلیون دلار رسیده است (جورجیادو[6] و همکاران، ۲۰۲۱). با این وجود، آنچه حتی نگران‌کننده‌تر است این است که پیش‌بینی می‌شود حملات خودی در آینده نزدیک افزایش یابد. واقعیت این است که شرایط بحرانی مشابه با شرایط فعلی (شیوع کووید-۱۹) منجر به ساختار کاری جدیدی با عنوان "دورکاری" یا "ترکیبی" می‌شود که در آن افراد تحت فشار داخلی و خارجی بیشتری قرار دارند (جورجیادو و همکاران، ۲۰۲۱).

به نظر می‌رسد که شرایط نه تنها سودمند نیست، بلکه در بسیاری از موارد، حوادث تهدید داخلی را با تدوین شرایط فنی، اجتماعی، اقتصادی و روانی مورد نیاز تسهیل می‌کند. بنابراین نقض امنیت داخلی به دلیل عدم شناسایی، پاسخ آهسته و روش‌های اصلاح ناسازگار به یک خطر تجاری بزرگ تبدیل می‌شود (لوکی[7] و همکاران، ۲۰۱۹) و این در حالی است که اکثر مردم تمایل دارند آسیب‌پذیری‌های سایبری را به عنوان یک مشکل تکنولوژیکی در نظر بگیرند و درک نمی‌کنند که بیشتر آسیب‌پذیری‌های امنیت سایبری اغلب نتیجه رفتار انسانی است. در یک زنجیره امنیتی معمولی، بسیاری از مردم متوجه نمی‌شوند که انسان ضعیف‌ترین و آسیب‌پذیرترین نقطه کل امنیت است. به عنوان مثال، کلاهبرداری‌های مهندسی اجتماعی، آشناترین رویکرد حمله سایبری، مبتنی بر هدف قرار دادن و دستکاری نقاط ضعف انسانیِ قربانیان احتمالی است. علاوه بر این، نگرش و رفتار انسان در این زنجیره امنیتی به طور قابل توجهی توسط فرهنگ او، که نظم ضمنی یک جامعه است، تعیین می‌شود (گرویسبرگ[8] و همکاران، ۲۰۱۸) و از سویی دیگر عوامل مرتبط با شخصیت افراد (گشودگی، وظیفه‌شناسی، برونگرایی، روان‌نژندی و توافق‌پذیری) نیز نقش پررنگی در این زنجیره امنیتی دارند (پاپاتساروچا[9] و همکاران، ۲۰۲۱).

در فرهنگی که هنجارها به دلیل فرهنگ جمعی قوی از اشتباه اجتناب می‌کنند، فردی که توسط کلاهبرداری مهندسی اجتماعی در معرض خطر قرار می‌گیرد ممکن است از ترس تنبیه شدن از این اشتباه خودداری کند. این امر مانع از واکنش به حادثه و تحقیقات بعدی در مورد حملات سایبری خواهد شد. علاوه بر این، انبوهی از راه‌حل‌های فن‌آوری برای تقویت زنجیره امنیتی، مانع از کلیک تصادفی یک فرد بر روی لینک دانلود بدافزار در شبکه نمی‌شود. زنجیره امنیتی به اندازه ضعیف‌ترین حلقه آن (که همان انسان است)، آسیب‌پذیر است.

1 - Deutrom
2 - Li
3 - Kumar & Nayar
4 - Naidoo
5 - Phonemon
6 - Georgiadou
7 - Luckey
8 - Groysberg
9 - Papatsaroucha

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

همراه با افزایش استفاده از دستگاه‌های تلفن همراه برای دسترسی به خدمات ضروری (مانند بانکداری، خرید آنلاین، خدمات دولتی و غیره) در اینترنت، مطالعه عوامل انسانی که منجر به آسیب‌پذیری‌های سایبری می‌شود، بسیار مهم است (هو[1]، ۲۰۲۱).

از جمله رویکردهای تقویت زنجیره امنیتی، فرهنگ‌سازی، افزایش آگاهی و آموزش است که هم مکانیسم امنیتی را که می‌توانند برای حفاظت از اطلاعات (معمولاً فناوری محور) اســـتفاده کنند و هم افزایش آگاهی آن‌ها از تهدیدات احتمالی زنجیره امنیتی را دربرمی‌گیرد (همان منبع). از ســویی دیگر، پژوهش‌ها نشــان داده اســت که آگاهی نســبت به این فضــا ارتباط تنگاتنگی با فرهنگ دارد (جورجیادو و همکاران، ۲۰۲۱؛ خاندو[2] و همکاران، ۲۰۲۱) بنابراین فرهنگ و آگاهی در حوزه امنیت ســایبری در قالب ســاختاری با عنوان «فرهنگ و آگاهی امنیتِ ســایبری» پدیدار می‌شود. از این‌رو، مساله‌ای که ذهن نگارندگان این سطور را درگیر نموده است، این امر است که عوامل روانشــناختی موثر بر فرهنگ و آگاهی امنیت ســایبری در دوره شــیوع کووید-۱۹، چه عواملی هســتند؟ بر پایه همین پرســش و با توجه به مقالات معتبر در حوزه فرهنگ و آگاهی امنیت ســایبری منتشــر شــده از ســال ۲۰۲۰ الی ۲۰۲۲ در داخل و خارج کشــور، تلاش شــد تا با استفاده از روش تحلیل مضمون[3]، این عوامل شناسایی و تفسیر شوند.

صفائی و قدیری (۱۳۹۹) در پژوهش خود تمام روندهای فعلی حملات امنیت سایبری در طی همه‌گیری و چگونگی تغییر حملات بین همه‌گیرهای مختلف را ارائه کرده، تاثیر کووید-۱۹ بر جامعه، از دیدگاه تهدید امنیت سایبری نیز بیان شده و بحث در مورد اینکه چرا آموزش امنیت سایبری هنوز از اهمیت بالایی برخوردار است، انجام گردید. نتایج حاصل از مصاحبه با خبرگان حوزه امنیت سایبری حاکی از آن بود که آموزش، وسیله اول در مورد چگونگی جلوگیری از تهدیدهای امنیت سایبری است.

اوپادهایای و راته[4] (۲۰۲۲) در پژوهشی بیان نمود کووید-۱۹ افق‌های جدیدی را برای یادگیری مجازی و فرهنگ دورکاری باز کرده است. اگرچه آموزش مجازی و جلسات برخط قبل از قرنطینه در دسترس بود، استفاده از این پلتفرم‌ها تشدید شده است. فقدان آگاهی در میان بسیاری از افراد در مورد خطرات استفاده از این پلتفرم‌ها وجود دارد که آن‌ها را مستعد حملات جرایم سایبری فیشینگ، سوءاستفاده جنسی یا کلامی، تمسخر و غیره می‌کند. شواهد نشان می‌دهد افزایش بی‌رویه جرایم سایبری در این مدت وجود داشته است. عدم آگاهی عمومی باعث شده است که افراد بی‌گناه طعمه مهاجمان شوند. از آنجایی که همه‌گیری و قرنطینه‌های متعاقب آن غافلگیرکننده بود، مقامات دولتی و خصوصی فرصتی برای ایجاد تمهیدات مناسب برای آموزش افراد و ایمن کردن این پلتفرم‌ها نداشتند. شکی نیست که اگر این پلتفرم ها ایمن شوند، به عنوان یک سرمایه برای جامعه ثابت خواهند شد، اما برای رسیدن به هدف امنیت کامل سایبری باید کار زیادی انجام شود.

عظمی[5] و همکاران (۲۰۲۱) در پژوهشی با هدف بررسی عوامل موثر بر فرهنگ امنیت اطلاعات در بین کارکنان شرکت‌های مخابراتی، با این انگیزه که افزایش تعداد حوادث نقض اطلاعات ناشی از کارکنان خودی سازمان‌ها بوده است بیان کردند یافته‌ها حاکی از آن بود که آموزش امنیت، برنامه‌های آموزش و آگاهی از امنیت اطلاعات تأثیر مثبت و قابل توجهی بر فرهنگ امنیت اطلاعات داشت. علاوه بر این، رفتار امنیتی گزارش شده کارکنان به عنوان یک واسطه جزئی در رابطه بین آگاهی از امنیت اطلاعات و فرهنگ امنیت اطلاعات عمل نمود.

همانطور که در مطالب پیشین اشاره شد، تحقیقات نشان داده است که ۳۰٪ از حوادث کلاهبرداری سایبری از آرامش به عنوان یک جذابیت احساسی استفاده می‌کنند (نایدو، ۲۰۲۰). به عنوان مثال، به منظور استفاده از امید به عنوان عنصر هیجانی برای جلب توجه قربانی هدف، مجرمان سایبری ممکن است اطلاعات نادرست در مورد درمان‌های احتمالی یا بودجه‌های امداد دولتی منتشر کنند. برای تسهیل ترس یا تهدید، ممکن است فشارهای مرتبط با کووید-۱۹، از جمله شیوع محلی را به گردش درآورند، یا از تصاویر ترسناک مرتبط با ویروس استفاده کنند تا قربانیان احساس آسیب‌پذیری و نگرانی کنند. همچنین ممکن است از لذت به عنوان یک جذابیت عاطفی برای تشویق قربانیان به خرید خدمات سرگرمی یا سوءاستفاده از شفقت مردم با درخواست کمک‌های مالی به افراد نیازمند استفاده کنند (نایدو، ۲۰۲۰). نتایج تحقیقات نشان می‌دهد که مجرمان سایبری تمایل دارند برای دستیابی به دستاوردهای پولی در طول این همه‌گیری کنونی، به ارسال درخواست‌های عاطفی مثبت به قربانیان هدف اعتماد کنند (ما و مک‌کینون، ۲۰۲۱). به طور کلی، باید گفت با توجه به اینکه در دوره شیوع کووید-۱۹، بخش اعظمی از فعالیت افراد (تدریس، دورکاری، ارتباطات اجتماعی و...) در فضای سایبری انجام می‌شود، رعایت

1 - Hoe
2 - Khando
3 - Thematic Analysis
4 - Upadhyay & Rathee
5 - Azmi

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

امنیت سایبری در دوره شیوع اهمیت پیدا کرده، بنابراین تشخیص مولفه‌های روانشناختی موثر در فرهنگ و آگاهی نسبت به امنیت سایبری و درک احساس افراد در طول یک بیماری همه‌گیر جهانی می‌تواند به محققان و متخصصان صنعت کمک می‌کند تا تصمیمات و انتخاب‌های فردی را بهتر درک کنند (لی، ۲۰۲۰) و راهکارهایی جهت ببود آنان ارائه نمایند. از این‌رو هدف از پژوهش حاضر بررسی عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید-۱۹ به روش تحلیل مضمون می‌باشد.

روش

پژوهش حاضر از نوع کیفی بوده و درصدد است تا با استفاده از روش تحلیل مضمون به گردآوری، تحلیل و تفسیر موضوع پژوهش (عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید-۱۹) اقدام نماید. این روش دارای شش گام است که به ترتیب عبارت از آشنا شدن با داده‌ها، کدگذاری اولیه، جستجو برای یافتن مضامین، بازبینی مضامین، تعریف و نامگذاری مضامین و تولید گزارش نهایی است (رجبی و همکاران، ۱۳۹۷). قابل ذکر است که روش تحلیل مضمون، طیف گسترده‌ای از فنون را دربرمی‌گیرد اما در این پژوهش با توجه به هدف و سوال پژوهش از تکنیک شبکه مضامین[1] استفاده شده است که در آن پژوهشگر داده‌ها را برای شناسایی مضامین بررسی نموده، مضامین پایه، سازمان‌دهنده و فراگیر را تشخیص داده و پس از آن، یک نقشه گرافیکی از ارتباط میان آن‌ها را نمایش می‌دهد. دلیل استفاده از تکنیک شبکه مضامین نیز این امر بوده است که پژوهشگران مقاله حاضر، قصد بر ارائه الگویی در ارتباط با عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری و پس از آن ساخت ابزار در این زمینه، دارند. بنابراین لازم است ابتدا به شیوه نظری مدل مفهومی اولیه طراحی گردد که در این مقاله این مساله مورد بررسی قرار می‌گیرد. قابل ذکر است که این شبکه‌ها صرفاً ابزاری تحلیلی هستند و نه خود تحلیل؛ وقتی یک شبکه مضمونی ساخته شد می‌توان از آن به مثابه ابزاری تصویری برای تفسیر متن استفاده کرد تا نتایج حاصل از متن و خود متن برای پژوهشگر و خوانندگان روشن شود (همان منبع). در این پژوهش جهت بررسی روایی، از روایی محتوی[2] به مدد خبرگان حوزه امنیت سایبری کشور استفاده شد. جهت اطمینان از اینکه مهم‌ترین و صحیح‌ترین محتوی (ضرورت آیتم) انتخاب شده است از شاخص نسبت روایی محتوی (CVR)[3] و برای اطمینان از این که آیتم‌های ابزار به بهترین نحو جهت اندازه‌گیری محتوی طراحی شده‌اند از شاخص روایی محتوی (CVI)[4] استفاده گردید. تعداد متخصصان در این بخش ۵ نفر بوده‌اند که روایی محتوی توسط آنان تایید شد. برای سنجش اعتبار[5] داده‌ها نیز از ضریب اعتبار هولستی[6] استفاده شد و مقدار آن بالاتر از ۰/۷ (۰/۸۶) بدست آمد که تایید کننده اعتبار بود.

برای انجام پژوهش حاضر، مجموعه مقالات منتشر شده در داخل و خارج کشور در حوزه فرهنگ و آگاهی امنیت سایبری، از زمستان ۱۳۹۸ شمسی معادل زمستان ۲۰۲۰ میلادی تا زمستان ۱۴۰۰ شمسی معادل زمستان ۲۰۲۲ میلادی (از زمان شیوع کووید-۱۹)، با ۴ کلیدواژه (فرهنگ، آگاهی، امنیت سایبری، عوامل روانشناختی) در پایگاه‌های سیویلیکا[7]، نورمگز[8]، مگ‌ایران[9]، گوگل‌اسکولار[10]، ساینس‌دایرکت[11] و آکادمیا[12] جمع‌آوری و در چارچوب نرم‌افزار MAXQDA مورد بررسی قرار گرفته است. مجموع مقالات در این حوزه ۱۱۶ مقاله (تعداد ۳۱ مقاله در داخل کشور و تعداد ۸۵ مقاله در خارج کشور) بوده است. از جمله معیارهای ورود مقالات به پژوهش محتوی قابل اجرا برای سوال پژوهش و مطالعات مربوط به متغیر هدف و معیارهای خروج خلاصه مقالات، فصل‌های کتاب، گزارش‌های شرکت و عدم دسترسی به متن کامل مقاله بوده است. بنابراین شناسایی، استخراج و کدگذاری پس از اعمال ملاک‌های خروج، از ۴۸ مقاله (۱۰

1 - Themes
2 - Content Validity
3 - Content Validity Ratio
4 - Content Validity Index
5 - Reliability
6 - Holsti's Cofficient of Reliability
7 - Civilica
8 - Noormags
9 - Magiran
10 - google scholar
11 - science direct
12 - academia

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

مقاله فارسی و ۳۸ مقاله انگلیسی) انجام شد و تعداد ۸۲۶ کد شناسایی گردید که پس از حذف کدهای تکراری و با تطبیق کدگذاری با کدگذاری دوم دستاورد آن (۴۸ کد) در جدول (۱) ارائه شده است.

یافته‌ها

کدگذاری اولیه

با بررسی مقالات حوزه فرهنگ و آگاهی امنیت سایبری، نکات کلیدی که به طور مستقیم یا غیرمستقیم با عوامل روانشناختی مرتبط بوده‌اند، استخراج شده که حاصل آن با ذکر منبع در جدول (۱) گزارش شده است.

جدول ۱. مجموعه مقالات فاقد طبقه‌بندی حوزه فرهنگ و آگاهی امنیت سایبری با تاکید بر عوامل روانشناختی

ردیف	منبع	نکات کلیدی
۱.	جورجیادو و همکاران (۲۰۲۱ب و پ، ت)، القمدی (۲۰۲۱)، اوچندو و همکاران (۲۰۲۱)	رفتار اعضاء به ویژه رفتار مدیران
۲.	اوگدن (۲۰۲۱)	خودکارآمدی، دانش و تجربه
۳.	الشیخ و آدامسون (۲۰۲۱)	دلبستگی
٤.	جورجیادو و همکاران (۲۰۲۱الف)	استرس عاطفی
٥.	دا-ویجا و همکاران (۲۰۲۲)، جورجیادو و همکاران (۲۰۲۱ الف،ب و پ)	رفتار امنیتی
٦.	کریم‌زاده و همکاران (۱۴۰۰)، جورجیادو و همکاران (۲۰۲۱الف)، ماشیان و کریتزینگر (۲۰۲۱)	هیجانات
۷.	کریم‌زاده و همکاران (۱۴۰۰)، رضوی و ساده میری (۱۳۹۹)، فراستی و ره پیک (۱۳۹۹)، خاندو و همکاران (۲۰۲۱)، پاولوا (۲۰۲۰)، جورجیادو و همکاران (۲۰۲۱الف)	افکار و باورها
۸.	جورجیادو و همکاران (۲۰۲۱الف)	درک خطر امنیتی
۹.	دا-ویجا و همکاران (۲۰۲۲)، جورجیادو و همکاران (۲۰۲۱ الف، ب و پ)، کواکویک و رادنکوویک (۲۰۲۰)، هاتزیواسیلیز و همکاران (۲۰۲۰)	آگاهی امنیتی
۱۰.	جورجیادو و همکاران (۲۰۲۱الف)	رویدادهای استرس‌زا و تهدیدات سایبری مرتبط با انسان
۱۱.	فراستی و ره پیک (۱۳۹۹)، دا-ویجا و همکاران (۲۰۲۲)، خاندو و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱الف، ب و پ)، اورهک و پتریک (۲۰۲۰)	نگرش
۱۲.	کولینز و هیندز (۲۰۲۱)	انگیزش درونی و بیرونی
۱۳.	کولینز و هیندز (۲۰۲۱)	تأثیرات اجتماعی و سازمانی
۱٤.	جورجیادو و همکاران (۲۰۲۱الف)، پاولوا (۲۰۲۰)	کار تیمی و گروهی
۱٥.	کریم‌زاده و همکاران (۱۴۰۰)، کریمی و همکاران (۱۴۰۰)، تولاه و همکاران (۲۰۲۱)، پاپاتساروچا و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱الف، ب و پ)	ویژگی‌های شخصیتی
۱٦.	کریم‌زاده و همکاران (۱۴۰۰)	جامعه‌پذیری ناقص و فرسایش سرمایه اجتماعی-خانوادگی
۱۷.	کریم‌زاده و همکاران (۱۴۰۰)	تغییرات سبک زندگی
۱۸.	کریم‌زاده و همکاران (۱۴۰۰)	ناکامی‌های اجتماعی
۱۹.	کریم‌زاده و همکاران (۱۴۰۰)	مدیریت نامناسب اوقات فراغت
۲۰.	کریم‌زاده و همکاران (۱۴۰۰)، صیادی‌تورانلو و همکاران (۱۳۹۹)	فقر فرهنگی
۲۱.	کریم‌زاده و همکاران (۱۴۰۰)	تنگناهای اقتصادی
۲۲.	کریم‌زاده و همکاران (۱۴۰۰)	فقدان قوانین به روز و کارآمد

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

۲۳.	کریم‌زاده و همکاران (۱۴۰۰)	جذاب نبودن برنامه‌های داخلی و نبود فضای مناسب برای تخلیه احساسات و هیجانات
۲٤.	فراشی و همکاران (۱۳۹۹)، صیادی‌تورانلو و همکاران (۱۳۹۹)	ناآگاهی و سطح پایین آگاهی
۲۵.	صیادی تورانلو و همکاران (۱۳۹۹)، اینکیستر (۲۰۲۱)	سلامت روان
۲٦.	رضوی و ساده میری (۱۳۹۹)	افشاگری
۲۷.	فراشی و همکاران (۱۳۹۹)	پایین بودن فرهنگ استفاده از فضای مجازی
۲۸.	فراشی و همکاران (۱۳۹۹)، جورجیادو و همکاران (۲۰۲۱الف)، پروگولاکیس و همکاران (۲۰۲۱)	نارضایتی کارکنان از فشار کاری و عدم تناسب نیروی انسانی با کار
۲۹.	پاپاتساروچا و همکاران (۲۰۲۱)، کوآیوم و همکاران (۲۰۲۱)، فراشی و همکاران (۱۳۹۹)، جورجیادو و همکاران (۲۰۲۱الف)	استفاده از گوشی هوشمند و رعایت نکردن ملاحظات امنیتی در محل کار
۳۰.	فراشی و همکاران (۱۳۹۹)، خاندو و همکاران (۲۰۲۱)	ضعف دانش کارکنان و آشنا نبودن به مباحث روز فناوری‌های نوین
۳۱.	ایسسر و برندتوینر (۲۰۲۲)؛ پری یادارشینی و همکاران (۲۰۲۱)؛ نرس (۲۰۲۱)؛ کوآیوم و همکاران (۲۰۲۱)؛ ماتیوکورهوا و همکاران (۲۰۲۱)	مهندسی اجتماعی
۳۲.	فورنل و شاه (۲۰۲۰)	عدم آمادگی
۳۳.	کوونتری و همکاران (۲۰۲۰)، خاندو و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱الف)، پروگولاکیس و همکاران (۲۰۲۱)	دسترسی از راه دور و کار در منزل
۳٤.	ماتیوکورهوا و همکاران (۲۰۲۱)، حسن و همکاران (۲۰۲۱)، کوونتری و همکاران (۲۰۲۰)، پاپاتساروچا و همکاران (۲۰۲۱)، الزبیدی (۲۰۲۱)، پری یادارشینی و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱ب و پ)، فورنل و شاه (۲۰۲۰)، گابرا و همکاران (۲۰۲۰)، هاتزیواسیلیز و همکاران (۲۰۲۰)، آبابا و لیزا (۲۰۲۰)	عدم رمزگذاری
۳۵.	صحرایی و همکاران (۱۳۹۹)، توکلی و همکاران (۱۳۹۹)، نگوین و همکاران (۲۰۲۲)، آدامو و همکاران (۲۰۲۲)، ایسسر و برندتوینر (۲۰۲۲)، دا-ویجا و همکاران (۲۰۲۲)، پاپاتساروچا و همکاران (۲۰۲۱)، پروگولاکیس و همکاران (۲۰۲۱)، اوچندو و همکاران (۲۰۲۱)، ممده و دابالا (۲۰۲۱)، گابرا و همکاران (۲۰۲۰)، آستانکوا (۲۰۲۰)، آبابا و لیزا (۲۰۲۰)	آموزش
۳٦.	کریم‌زاده و همکاران (۱۴۰۰)، رضوی و ساده‌میری (۱۳۹۹)، فراشی و همکاران (۱۳۹۹)، ذاکری‌هامانه و همکاران (۱۳۹۹)، ایسسر و برندتوینر (۲۰۲۲)، پاپاتساروچا و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱ب و پ)، کوآیوم و همکاران (۲۰۲۱)، بوتاویکیوس و همکاران (۲۰۲۰)	اعتماد
۳۷.	فراشی و همکاران (۱۳۹۹)، کاویانی و همکاران (۱۳۹۹)، خاندو و همکاران (۲۰۲۱)، جورجیادو و همکاران (۲۰۲۱الف، ب و پ)، آستانکوا (۲۰۲۰)	شایستگی کارکنان
۳۸.	فراشی و همکاران (۱۳۹۹)؛ صحرایی و همکاران (۱۳۹۹)؛ اوچندو و همکاران (۲۰۲۱)	توانایی پاسخگویی به تهدید
۳۹.	نگوین و همکاران (۲۰۲۲)؛ پاپاتساروچا و همکاران (۲۰۲۱)؛ العلوی و الباسام (۲۰۲۱)؛ اوچندو و همکاران (۲۰۲۱)؛ اورهک و پتریک (۲۰۲۰)؛ آبابا و لیزا (۲۰۲۰)	تعهد

جستجو برای یافتن مضامین

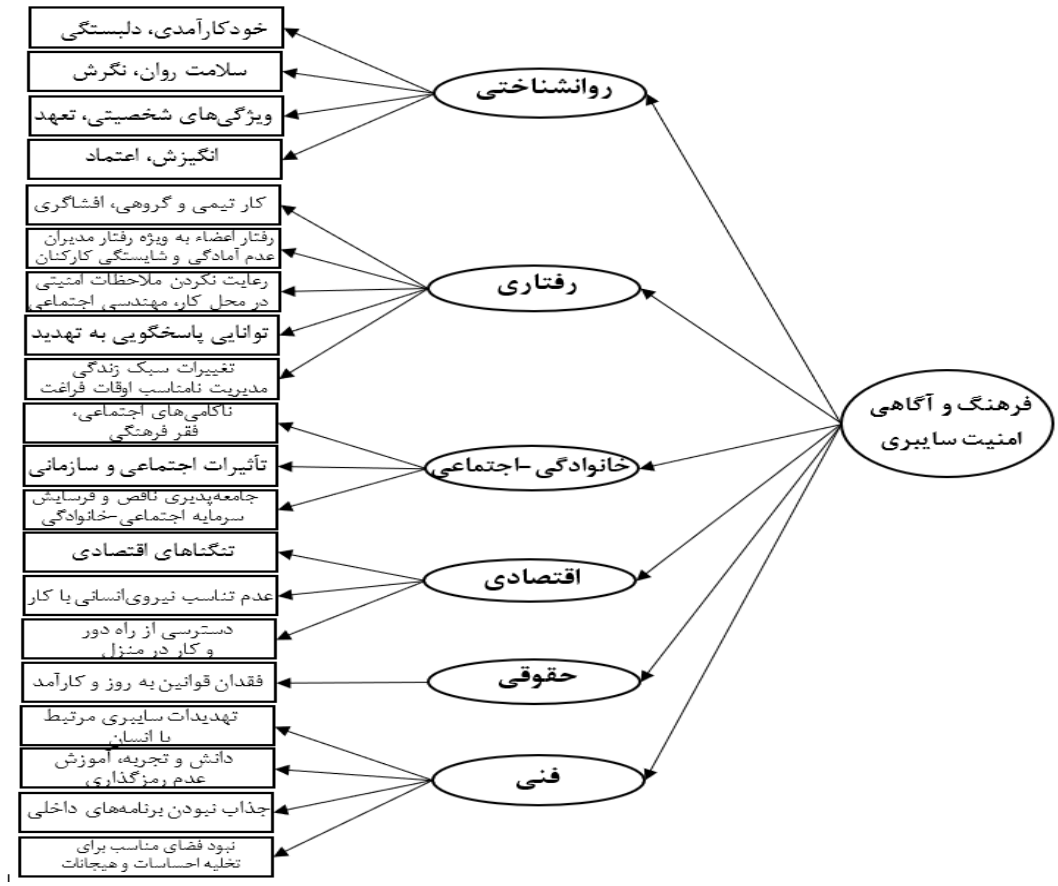
در این مرحله، تلاش می‌شود تا کدهای بدست آمده از مرحله پیشین ذیل مضامین پایه، سازمان دهنده و فراگیر طبقه‌بندی گردند. جدول شماره (۲)، نمایی از این تلاش را ترسیم نموده است.

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

جدول ۲. مضامین پایه، سازمان‌دهنده و فراگیر فرهنگ و آگاهی امنیت سایبری

مضمون فراگیر	مضامین سازمان دهنده	مضامین پایه
فرهنگ و آگاهی امنیت سایبری (۴۵ مضمون)	**روانشناختی** (۱۶ مضمون)	خودکارآمدی، دلبستگی، سلامت روان (استرس عاطفی، هیجانات، افکار و باورها، رویدادهای استرس‌زا)، نگرش (درک خطر امنیتی، آگاهی امنیتی)، انگیزش (درونی و بیرونی)، ویژگی‌های شخصیتی، اعتماد، تعهد.
	رفتاری (۱۱ مضمون)	رفتار اعضاء به ویژه رفتار مدیران، رفتار امنیتی، کار تیمی و گروهی، تغییرات سبک زندگی، مدیریت نامناسب اوقات فراغت، افشاگری، استفاده از گوشی هوشمند و رعایت نکردن ملاحظات امنیتی در محل کار، عدم آمادگی، شایستگی کارکنان، توانایی پاسخگویی به تهدید، مهندسی اجتماعی.
	خانوادگی-اجتماعی (۵ مضمون)	تأثیرات اجتماعی و سازمانی، جامعه‌پذیری ناقص و فرسایش سرمایه اجتماعی-خانوادگی، ناکامی‌های اجتماعی، فقر فرهنگی.
	اقتصادی (۵ مضمون)	تنگناهای اقتصادی، نارضایتی کارکنان از فشار کاری و عدم تناسب نیروی انسانی با کار، دسترسی از راه دور و کار در منزل.
	حقوقی (۱ مضمون)	فقدان قوانین به روز و کارآمد
	فنی (۵ مضمون)	دانش و تجربه، تهدیدات سایبری مرتبط با انسان، عدم رمزگذاری، آموزش، جذاب نبودن برنامه‌های داخلی و نبود فضای مناسب برای تخلیه احساسات و هیجانات

جمع‌بندی از جدول (۲) را می‌توان در قالب شبکه مضامین در شکل (۱) ترسیم نمود.



شکل ۱. شبکه مضامین عوامل موثر در فرهنگ و آگاهی امنیت سایبری

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

مطابق یافته‌ها، عوامل موثر در فرهنگ و آگاهی امنیت سایبری در ۶ دسته عوامل روانشناختی، رفتاری، خانوادگی-اجتماعی، اقتصادی، حقوقی و فنی تقسیم‌بندی می‌شوند و در شکل (۱) برای هر عامل، نمونه مثال ذکر شده است. براساس شبکه ارائه شده در شکل (۱) و نیز با توجه به جدول (۱)، مولفه‌هایی که در پژوهش‌ها بیشترین توجه را به خود جلب کرده‌اند، مربوط به عوامل روانشناختی و شامل مواردی همچون خودکارآمدی، دلبستگی، سلامت روان (استرس عاطفی، هیجانات، افکار و باورها، رویدادهای استرس‌زا)، نگرش (درک خطر امنیتی، آگاهی امنیتی)، انگیزش (درونی و بیرونی)، ویژگی‌های شخصیتی، اعتماد و تعهد بودند.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف شناسایی عوامل روانشناختی موثر بر فرهنگ و آگاهی امنیت سایبری در دوره شیوع کووید-۱۹ با استفاده از اسناد بالادستی و رویکرد تحلیل مضمون انجام گرفته است. با کمی تامل در مولفه‌های ارائه شده در جدول (۱) و شکل (۱)، متوجه می‌شویم که شمار زیادی از این مولفه‌ها تحت تاثیر متغیرهای روانشناختی همچون خودکارآمدی، دلبستگی، سلامت روان، نگرش، انگیزش، ویژگی‌های شخصیتی، اعتماد و تعهد بوده و در این بین پررنگ‌ترین آن‌ها ویژگی‌های شخصیتی هستند که ارتباط پررنگی با سایر متغیرهای روانشناختی ذکر شده، دارند. ویژگی گشودگی به تجربه[1]، که به تمایل افراد به داشتن ذهنی باز نسبت به ایده‌ها و تجربیات جدید و پذیرش باورهای مختلف اشاره دارد نشان می‌دهد افرادی که امتیاز بالایی در آن دارند، درک بالایی از هنر، افزایش تخیل و اشتیاق برای ماجراجویی نشان می‌دهند. از سوی دیگر، افرادی که امتیاز پایینی دارند، در کارهای روزمره خود احساس راحتی بیشتری می‌کنند و به دنبال تجربیات جدید نیستند. وظیفه‌شناسی[2] نیز شامل ویژگی‌هایی مانند صداقت، اعتماد، خودمداری قوی و مسئولیت‌پذیری است و افرادی که امتیاز بالایی در این ویژگی دارند، بیشتر به برنامه‌ها پایبند هستند و از قوانین پیروی می‌کنند (پاپاتساروچا و همکاران، ۲۰۲۱).

برون‌گرایی شاخص دیگری است که به مهارت‌های اجتماعی مربوط می‌شود و افرادی که امتیاز بالایی در این ویژگی دارند در گروه‌های بزرگی از مردم احساس راحتی می‌کنند و تمایل دارند که مشتاق، پرانرژی و پرحرف باشند. برعکس، افرادی که در این ویژگی امتیاز پایینی دارند را می‌توان درون‌گرا توصیف کرد و بنابراین، ممکن است در گروه‌های کوچک‌تری از افراد احساس راحتی بیشتری داشته باشند. توافق‌پذیری نیز افرادی را توصیف می‌کند که بیشتر به دیگران کمک می‌کنند و به آن‌ها اعتماد می‌کنند، زیرا آن‌ها همیشه بهترین را در افراد دیگر فرض می‌کنند. بسته به اینکه یک فرد چقدر در این ویژگی نمره بالا یا پایین می‌گیرد، موافق بودن می‌تواند معیاری برای مهربانی و شفقت باشد. روان‌رنجوری آخرین الگوی شخصیتی است که به افزایش سطح اضطراب اشاره دارد. هر چه فردی در این ویژگی امتیاز بیشتری کسب کند، بیشتر تمایل به نگرانی دارد، در حالی که نمرات پایین‌تر نشان‌دهنده ثبات عاطفی است. بنابراین با دانستن مقدار نمره افراد در خصوص این ویژگی‌ها می‌توان برنامه‌های آموزشی مرتبط با فرهنگ و آگاهی امنیت سایبری را به گونه دقیق‌تری تنظیم نمود، چرا که ویژگی‌های شخصیتی می‌تواند به عنوان شاخصی از قصد رفتاری مرتبط با امنیت سایبری کاربران در رابطه با دستگاه‌های رایانه‌ای عمل کند. به عنوان مثال افراد روان‌رنجورخو، به شدت نگران امنیت و حریم خصوصی خود هستند و این امر ممکن است حساسیت به حملات سایبری مانند فیشینگ را کاهش دهد (همان منبع).

طبق یافته‌های گزارش شده در جدول (۱) شخصیت در پژوهش‌های سه سال اخیر مرتبط با فرهنگ و آگاهی امنیت سایبری (کریم‌زاده و همکاران، ۱۴۰۰؛ کریمی و همکاران، ۱۴۰۰؛ تولاه و همکاران، ۲۰۲۱؛ پاپاتساروچا و همکاران، ۲۰۲۱؛ جورجیادو و همکاران، ۲۰۲۱الف، ب و پ) هم در داخل کشور و هم در خارج کشور، مورد بحث قرار گرفته است و انتشار این پژوهش‌ها حاکی از این است که در نظر گرفتن شخصیت در متون مرتبط با فرهنگ و آگاهی امنیت سایبری در حال افزایش است. نگرانی بالقوه در این جهت مربوط به حریم خصوصی خود کارکنان است. برای مثال، جمع‌آوری اطلاعات شخصیتی می‌تواند در ایجاد برنامه‌های فرهنگ امنیت سایبری سفارشی‌شده‌تر در سازمان‌ها مفید باشد، اما نگرانی‌های مربوط به حریم خصوصی کارمندان می‌تواند منجر به عدم تمایل افراد به اشتراک‌گذاری چنین اطلاعات شخصی با کارفرمای خود شود (تولاه و همکاران، ۲۰۱۹؛ دا-ویجا و همکاران، ۲۰۲۰).

در واقع درست است که فرهنگ امنیت سایبری نسبتاً جدیداً ظهور کرده است، اما این در حالی است که در دهه گذشته به یک اصطلاح تثبیت شده در صنعت و رسانه همراه با اصطلاحاتی مانند حمله سایبری، تهدید سایبری و جاسوسی سایبری تبدیل شده است. در این

1 - Openness to experience
2 - Conscientiousness

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

راستا تحقیقات نشان می‌دهد که تمایلات رفتاری کارکنان مهم بوده و با بررسی جنبه‌های انسانی، سازمان‌ها باید رویکرد سفارشی‌تری به فرهنگ امنیت سایبری داشته باشند و پیشنهاد می‌کند که کارکنان در شرکت از دیدگاه روانشناختی بیشتری ارزیابی شوند و به مفاهیمی مانند شخصیت، علایق، نیازها و انگیزه‌ها توجه کنند (وانت ووت[1]، ۲۰۱۹).

به طور کلی به منظور اندازه‌گیری سطح فرهنگ و آگاهی امنیت سایبری و یا ارزیابی آن لازم است که سازمان‌ها متغیرهای روانشناختی بخصوص شخصیت و سلامت روان را در نظر داشته باشند و با توجه به عوامل شناسایی شده در پژوهش حاضر، تصمیمات و رویکردهایی را در جهت برطرف نمودن عوامل منفی بکار گیرند. چراکه این مولفه‌ها باید در جایی که منابع اجازه می‌دهند مورد آزمایش و مشاهده قرار گیرند، زیرا این کار دقیق‌ترین ارزیابی را از وضعیت فرهنگ و آگاهی امنیت سایبری ارائه می‌دهد. از این‌رو پیشنهاد می‌شود ابزاری منطبق با عوامل شناسایی شده در پژوهش حاضر تنظیم و براساس فرهنگ کشور عزیزمان ایران، بومی‌سازی گردد تا از طریق آن بتوان سطح فرهنگ و آگاهی افراد به خصوص کارکنان شاغل در بخش‌های خصوصی و دولتی که با سرمایه کشور به هر نحوی در ارتباط بوده و کوچکترین خطایی از سوی آنان منجر به آسیب‌های مالی و شاید هم جانی جبران‌ناپذیری به مردم شود، ارزیابی نمود و با اتخاذ تصمیمات و راهکارهایی مفید و مثمره ثمر کمک شایانی به آگاه‌سازی افراد در حوزه امنیت سایبری نمود.

با توجه به اینکه در پژوهش حاضر از روش تحلیل مضمون و بررسی مقالات منتشر شده در سه سال اخیر استفاده شده است، از جمله مهم‌ترین محدودیت‌های روش‌شناختی پیش‌روی پژوهشگران این مقاله مواردی همچون محدودیت زمانی به منظور دسته‌بندی عوامل شناسایی شده و نیز عدم دسترسی به برخی مقالات بسیار قوی (اکثر مقالات مربوط به سال ۲۰۲۲) در این حوزه اشاره نمود.

منابع

توکلی، ف.، مرتضوی، س.م.، کشاورزترک، م. (۱۳۹۹). تعیین عوامل راهبردی مؤثر بر پیشگیری از جرایم سایبری با رویکرد دلفی فازی. *فصلنامه انتظام اجتماعی*، ۱۲(۴): ۱۱۳-۱۴۰. DOR:20.1001.1.20086024.1399.12.4.5.8

ذاکری‌هامانه، ر.، اعظم‌آزاده، م.، قاضی‌نژاد، م.، باستانی، س. (۱۳۹۹). بررسی کیفی احساس امنیت آنلاین کاربران شبکه‌های اجتماعی. *مطالعات رسانه‌های نوین*، ۶(۲۱)، ۱۴۱-۱۷۸. 10.22054/nms.2020.42506.741

رحیم‌اف، ه.، موحدی صفت، م.ر. (۱۳۹۹). الگوی راهبردیِ ارزیابیِ عملیاتِ سایبری. *فصلنامه مدیریت نظامی*، ۲۰(۸۰)، ۳۱-۶۴. : 10.22034/iamu.2021.137430.2462

رجبی، م.، رجبی، ه.، احمدآبادی، م. (۱۳۹۷). تحلیل مضمون الزامات تحققِ امنیت انتظامی در اندیشه فرماندهی معظم کل قوا(مدظله‌العالی). *فصلنامه انتظام اجتماعی*، ۱۰(۲)، ۸۵-۱۰۸.http://sopra.jrl.police.ir/article_94576.html

رضوی، س.ی.، ساده‌میری، ج. (۱۳۹۹). مؤلفه‌های تأثیرگذار در ارتقای سطح هوشیاری و هوشمندی کارکنان ناجا در برابر تهدیدها و آسیب‌های جنگ نرم (مبتنی بر منظومه فکری امام خامنه‌ای(مدظله‌العالی)). *فصلنامه مطالعات حفاظت و امنیت انتظامی*، ۱۵(۵۵)، ۷۷-۴۳. http://spaps.jrl.police.ir/article_94797.html

صحرایی، م.، ولوی، م.ر.، بیات، ب.، ترقی، ع. (۱۳۹۹). ارائه مدل بومی رصد، پایش و هشداردهی سایبری براساس چرخه اودا. *فصلنامه علمی امنیت ملی*، ۱۰(۳۷)، ۵۱۲-۴۷۳. 1001.1.33292538.1399.10.37.15.8

صفائی، ع.، قدیری، م. (۱۳۹۹). تاثیرات همه‌گیری Covid-19 در حوزه امنیت سایبری، *هفتمین همایش سراسری علوم و مهندسی دفاعی سپاه*،تهران، https://civilica.com/doc/1235551

صیادی‌تورانلو، ح.، میرغفوری، س.ح.، مهدوی، م.ر.، ثقفی، س. (۱۳۹۹). تحلیل عوامل مرتبط بر ایجاد جرائم فضای مجازی با گوشی از رویکرد فازی. *پژوهشنامه نظم و امنیت انتظامی*، ۱۳(۵۱)، ۵۴-۲۷. 10.22034/osra.2020.94388

عابدی، ا. (۱۳۹۸). بررسی مفهوم امنیت سایبری، *دومین کنفرانس ملی پدافند سایبری،مراغه*، https://civilica.com/doc/903740

فراستی، ا.، ره‌پیک، س. (۱۳۹۹). بررسی تأثیر مؤلفه‌های پیشگیرانه بر کنترل و کاهش ارتکاب جرائم کارکنان پایور نیروهای مسلح. *فصلنامه علمی امنیت ملی*، ۱۰(۳۵)، ۳۲۶-۲۹۱. 20.1001.1.33292538.1399.10.35.11.0

فراشی، ا.ر.، استرکی، ا.، عبیری، د. (۱۳۹۹). صیانت از مأموریت‌های سایبری در سازمان‌های امنیتی. *فصلنامه مطالعات حفاظت و امنیت انتظامی*، ۱۵(۵۵)، ۱۶۰-۱۲۹. http://spaps.jrl.police.ir/article_94799.html

1 - Van't Wout

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

قربان‌پور، ع.، قربان‌پور، م. (۱۳۹۷). مفهوم امنیت ملی و نقش قانون اساسی جمهوری اسلامی ایران در تامین آن، *نخستین جشنواره تالیفات علمی برتر علوم انسانی اسلامی جایزه ویژه علامه جعفری*، https://www.sid.ir/fa/seminar/ViewPaper.aspx?ID=95186

کاویانی، ح.، میرسپاسی، ن.، معمارزاده‌طهران، غ.ر. (۱۳۹۹). طراحی مدل شایستگی کارکنان در حوزه امنیت سایبری. *مطالعات بین‌رشته‌ای دانش راهبردی*، ۱۰(۴۱)، ۲۹۸-۲۷۳. 20.1001.1.24234621.1399.10.41.11.7

کریم‌زاده، ب.، پورقهرمانی، ب.، بیگی، ج. (۱۴۰۰). طراحی مدل بومی سرمایهٔ اجتماعی برای پیشگیری از جرائم سایبری. *فصلنامه انتظام اجتماعی*، ۱۳(۲)، ۱۴۸-۱۱۵. DOR:20.1001.1.20086024.1400.13.2.5.1

کریمی، ز.، کاوه، م.، صالحی، ر.، ملتجی، م. (۱۴۰۰). بررسی نقش شخصیت و متغیرهای فردی بر نقض امنیت رمز عبور: یک مطالعه تجربی، *دوفصلنامه فناوری اطلاعات و ارتباطات ایران*، ۱۳ (۴۹ و ۵۰): ۱۷۳-۱۸۲. 20.1001.1.27170414.1400.13.49.8.8

Adamu, A. G., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering*, 12(1), 572-584. DOI:10.11591/ijece.v12i1.pp572-584

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

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*. In press https://doi.org/10.1016/j.matpr.2021.04.093

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829-841. https://link.springer.com/article/10.1007/s00779-021-01551-2

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), 1-8. https://doi.org/10.1016/j.heliyon.2021.e06016

Azmi, N. A. A. M., Teoh, A. P., Vafaei-Zadeh, A., & Hanifah, H. (2021). Predicting information security culture among employees of telecommunication companies in an emerging market. *Information & Computer Security*. 29 (5), 866-882. https://doi.org/10.1108/ICS-02-2021-0020

Collins, E. I., & Hinds, J. (2021). Exploring workers' subjective experiences of habit formation in cyber-security: A qualitative survey. *Cyberpsychology, Behavior, and Social Networking*. 24(9):599-604 https://doi.org/10.1089/cyber.2020.0631

Da-Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, 1-52. https://doi.org/10.1016/j.cose.2020.101713

Da-Veiga, A., Loock, M., & Renaud, K. (2022). Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. *The Electronic Journal of Information Systems in Developing Countries*, *88*(1), 1-19. https://doi/abs/10.1002/isd2.12198

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in human behavior*, *108*, 1-37. https://doi.org/10.1016/j.chb.2020.106310

Deutrom, J., Katos, V., & Ali, R. (2021). Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19. *Behaviour & Information Technology*, 1-15. doi.org/10.1080/0144929X.2021.1973107

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

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021b). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 1-20. doi: 10.1057/s41284-021-00286-2

Groysberg, B., Lee, J., Price, J., & Cheng, J. (2018). The leader's guide to corporate culture. *Harvard business review*, *96*(1), 44-52. https://www.hbs.edu/faculty/Pages/item.aspx?num=53726

Gunawan, B., & Ratmono, B. M. (2020). Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace. *Int. J. Netw. Secur.*, *22*(1), 93-101. DOI : 10.6633/IJNS.202001_22(1).09

Hakak, S., Khan, W. Z., Imran, M., Choo, K.-K. R., & Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. IEEE Access, 8, 124134–124144. doi.org/10.1109/ACCESS.2020.3006172

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 1-16. https://doi.org/10.1016/j.jisa.2020.102726

HOE, K. W. (2021). *Culture and cyber security: How cultural tightness-looseness moderates the effects of threat and coping appraisals on mobile cyber hygiene*. Singapore Management University, Dissertations and Theses Collection, 1-121. https://ink.library.smu.edu.sg/etd_coll/357/

Inkster, B. (2021). Cybersecurity: A Critical Priority for Digital Mental Health. 36, 18-29. 10.31234/osf.io/p9u3g 10.31234/osf.io/p9u3g

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 1-22. https://doi.org/10.1016/j.cose.2021.102267

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]

Kumar, A., & Nayar, K. R. (2020). COVID 19 and its Mental Health Consequences. Journal of Mental Health, 30 (1), 1–2. https://doi.org/10.1080/09638237.2020.1757052

Luckey, D., Stebbins, D., Orrie, R., Rebhan, E., Bhatt, S. D., & Beaghley, S. (2019). *Assessing continuous evaluation approaches for insider threats: How can the security posture of the US departments and agencies be improved*. RAND Corporation Santa Monica United States. 1-87. https://www.rand.org/pubs/research_reports/RR2684.html

Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*. 29(2), 433-446. doi.org/10.1108/JFC-01-2021-0016

Mamade, B. K., & Dabala, D. M. (2021). 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*,1, 699-724. https://doi.org/10.13052/jcsm2245-1439.1044

Mashiane, T., & Kritzinger, E. (2021). Identifying behavioral constructs in relation to user cybersecurity behavior. *Eurasian Journal of Social Sciences*, 9(2), 98-122. https://econpapers.repec.org/article/ejnejssjr/v_3a9_3ay_3a2021_3ai_3a2_3ap_3a98-122.htm

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy*, *4*(2), 141-152. https://doi.org/10.1002/spy2.141

Naidoo, R. (2020). A Multi-Level Influence Model of COVID-19 Themed Cybercrime. European Journal of Information Systems, 29(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

Nurse, J. R. (2021). Cybersecurity Awareness. *arXiv preprint arXiv*.1, 1-5. https://doi.org/10.1007/978-3-642-27739-9 1596-1

Ogden, S. E. (2021). *CYBERSECURITY: CREATING A CYBERSECURITY CULTURE*. Electronic Theses, Projects, and Dissertations, California State University - San Bernardino, 1-182 https://scholarworks.lib.csusb.edu/etd/1284/

Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. *Information & Computer Security*. 29 (1), 133-158. https://doi/10.1108/ICS-12-2019-0140/full/html

Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., Pallis, E., & Markakis, E. (2021). A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues. *arXiv preprint arXiv:2106.09986*. 1-39. https://doi.org/10.48550/arXiv.2106.09986

Pavlova, E. (2020). Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation. *Information & Security*, *46*(3), 239-249. https://doi.org/10.11610/isij.4617

Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K., & Satapathy, S. C. (2021). Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering*, *93*, 1-15. https://doi.org/10.1016/j.compeleceng.2021.107204

Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D., & Karamperidis, S. (2021). Perspectives on Cyber Security for Offshore Oil and Gas Assets. *Journal of Marine Science and Engineering*, *9*(2), 90-112. https://doi.org/10.3390/jmse9020112

Rothan, H. A., & Byrareddy, S. N. (2020). The Epidemiology and Pathogenesis of Coronavirus Disease (COVID-19) Outbreak. *Journal of Autoimmunity*, 109, 1-4. doi.org/10.1016/j.jaut.2020.102433

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An Empirical Analysis of the Information Security Culture Key Factors Framework. *Computers & Security*, 108, 1-37. https://doi.org/10.1016/j.cose.2021.102354

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 1-23. https://doi.org/10.1016/j.cose.2021.102387

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., & Fitriana, R. (2019). Cybercrime case as impact development of communication technology that troubling society. *Int. J. Sci. Technol. Res*, *8*(9), 1224-1228. https://publons.com/publon/27365038/

Upadhyay, N. K., & Rathee, M. (2022). Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Medicine, Law & Society*, *15*(1), 89-106. doi.org/10.18690/mls.15.1.89-106.2022

Van't Wout, C. (2019). Develop and maintain a cybersecurity organisational culture. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS*, 457, 36-49. http://hdl.handle.net/10204/11345

[Downloaded from frooyesh.ir on 2026-11-08]
[DOR: 20.1001.1.2383353.1401.11.6.11.8]