«پدافند الکترونیکی و سایبری»
سال دوازدهم، شماره ۳، فصل پاییز ۱۴۰۳؛ ص ۳۵-۲۵

علمی – پژوهشی

نقش آگاهی از امنیت اطلاعات کارکنان در پیشگیری از حملات مهندسی اجتماعی [نمونه موردی: کارمندان شهرداری تهران]

سید حسن حسینی[۱]، نسیم مجیدی*[۲]

۱- دانشجوی دکتری، ۲-عضو هیئت علمی، دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران

(دریافت: ۱۴۰۳/۰۲/۲۷، بازنگری: ۱۴۰۳/۰۶/۰۹، پذیرش: ۱۴۰۳/۰۷/۰۶، انتشار: ۱۴۰۳/۰۸/۰۱)

DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.4.6

چکیده

مهندسی اجتماعی شکلی از حمله است که به دنبال فریب کارکنان برای افشای اطلاعات محرمانه‌شان یا اجرای اقداماتی از جانب آنان است که امنیت سازمان را تهدید می‌کند. هدف این مقاله مطالعه عوامل سازمانی و فردی است که بر آگاهی از امنیت اطلاعات کارکنان تأثیرگذار بوده و این که چگونه این موجب پیشگیری از حملات مهندسی اجتماعی می‌شود. این تحقیق بر روی ۱۳۲۲ نفر از کارکنان شهرداری تهران انجام گرفته است. آگاهی از امنیت اطلاعات به عنوان یکی از عوامل اصلی در تأمین امنیت اطلاعات و ارتقای سطح آگاهی امنیت اطلاعات به عنوان یک عامل مهم در حفاظت از سازمان در برابر حملات احتمالی تأیید گردید. نظریه عمل منطقی و نظریه بسط‌یافته آن یعنی نظریه رفتار برنامه‌ریزی شده در این مطالعه مورد استفاده قرار گرفت. ۱۲ فرضیه بر اساس نظرات کارشناسان و تحقیقات قبلی صورت گرفته طراحی شد که پیمایش صورت گرفته نشان داد که شش مورد از فرضیات تأیید، سه مورد از آنها تا حدودی تأیید و سه مورد از آنها رد شدند. نتایج تحقیق نشان داد که سیاست‌های امنیت اطلاعات، برنامه‌های آگاه‌سازی، آموزشی و مهارت‌افزایی امنیتی و تأثیر آگاه‌سازی بر بینش و انگیزه کارکنان و تاثیر کنترل رفتار ادراکی بر انگیزه کارکنان در مقابله با مهندسی اجتماعی تأثیرات معناداری در پیشگیری از وقوع مهندسی اجتماعی دارد. ارتباط رهبری، اعتماد و رفتارهای پرخطر با موضوع آگاهی از امنیت اطلاعات نیز سنجش و ارتباط ضعیفی میان آنها یافت گردید.

کلیدواژه‌ها: آگاهی از امنیت اطلاعات، مهندسی اجتماعی، هنجار ذهنی، کنترل رفتار ادراکی، سیاست‌های امنیت اطلاعات

۱- مقدمه

اهمیت روزافزون اطلاعات دیجیتال نه‌تنها فرصت‌هایی را ایجاد کرده؛ بلکه تهدیدات امنیتی را نیز با خود به همراه دارد. گسترش بن سازه‌های شبکه‌های اجتماعی مهاجمان را قادر ساخته تا داده‌های شخصی کارکنان را از طریق ردّپاهای برخط آنها جمع‌آوری کنند. اطلاعات حاصله از این طریق می‌تواند برای تسهیل حملات انجام‌گرفته بر روی سازمان‌ها به کار گرفته شود [۱]. ازآنجایی‌که انسان‌ها در فرایند تصمیم‌سازی دخیل است و مسئولیت‌های مختلفی را بر عهده دارند عامل انسانی یک عامل بسیار مهم در امنیت اطلاعات محسوب می‌شود [۲]. حتی قوی‌ترین ابزارهای حفاظتی فنی درصورتی‌که مهاجم بتواند بر روی کارکنان اثرگذاری کند کارایی ندارند [۳]. مهندسی اجتماعی شکلی از حمله است که در آن افراد به‌صورت ارادی فریب‌خورده یا مورد سوءاستفاده واقع شده تا اطلاعات محرمانه را افشا کرده یا اقدامات مورد نظر مهاجم را انجام دهند که این اقدامات می‌تواند امنیت فرد یا سازمان را تهدید کند [۴]. حملات مهندسی اجتماعی شامل ابعاد فنی، اجتماعی و فیزیکی شده که در مراحل مختلف حمله مورد استفاده قرار می‌گیرند. حتی اگر چنین حمله‌ای در ابتدا ناموفق باشد، داشتن اطلاعات فردی یا سازمانی یا اطلاع از فرایندهای امنیت‌سازمانی و فردی می‌تواند برای حملات آتی مورداستفاده قرار گیرد [۵].

با این وجود، در خصوص موضوع مهندسی اجتماعی

* رایانامه نویسنده مسئول: nas.majidi_gahrodi@iauctb.ac.ir

پژوهش‌های بسیار اندکی در داخل کشور صورت‌گرفته که یکی از دلایل آن میان‌رشته‌ای بودن این موضوع است که سبب چندوجهی شدن و به تبع آن پیچیدگی پرداختن به آن می‌شود. این پژوهش نیز از معدود تحقیقات صورت‌گرفته در زمینه مهندسی اجتماعی است. مهندسان اجتماعی از روش‌هایی مثل اسپیرفیشینگ[1] [۶-۸] ، دستاویزسازی [۶ و ۹]، زباله‌گردی [۷]، سرک‌کشی [۷ و ۹]، مهندسی‌اجتماعی معکوس [۶ و ۷]، حفاری‌آب [۷]، طعمه‌گذاری [۷] یا جعل‌هویت کارکنان [۶ و ۹] برای دستیابی به اطلاعات شخصی یا سیستم‌های امن استفاده می‌کنند. این روشها را می‌توان به چهار دسته روشهای فنی که مبتنی بر ابزارهای فنی بوده، روش‌های فیزیکی که نیازمند اقدام فیزیکی از جانب مهاجم بوده، روشهای اجتماعی که نیازمند تعامل اجتماعی با قربانی و روشهای فنی-اجتماعی که نیازمند توأمان روشهای فنی و اجتماعی بوده تقسیم کرد [۴۰].روشهای مقابله با حملات مهندسی اجتماعی را می‌توان به سه بخش پیشگیری، کشف و خنثی‌سازی تقسیم کرد. در حوزه پیشگیری دو راهبرد وجود دارد: انسان‌محور و فناوری‌محور. راهبردهای انسان‌محور شامل اجرای سیاست‌ها و فرایندها در سازمان و نیز برنامه‌های آگاه‌سازی و آموزش کارکنان می‌شود. راهبردهای فناوری‌محور شامل پایش وب‌سایت، نصب دیواره‌آتش و ... می‌شود. روش کشف را نیز می‌توان به روشهای کشف انسانی و فناورانه تقسیم کرد. روشهای کشف انسانی شامل استفاده از انسان‌ها به عنوان حس‌گرهای امنیتی، پوشش‌های امنیتی پویا و ارزیابی خطر مبتنی بر مهندسی اجتماعی بوده و روشهای فناورانه کشف شامل کشف صفحات وب شبیه فیشینگ با استفاده از ابزارهای حفاظت در برابر جعل‌هویت می‌شود. روشهای خنثی‌سازی شامل کشف حساب‌های رسانه‌های اجتماعی جعلی، هشداردهی در خصوص رسانه‌های اجتماعی، ابزارهای مقابله با جاسوس‌افزار، آگاه‌سازی امنیتی افراد و سازمان‌ها و ابزارهای مقابله با کلاهبرداری‌های بانکی می‌شود [۳۹].کارکنانی که دانش کافی در مورد خطرات مهندسی اجتماعی ندارند، بزرگترین آسیب برای سازمان محسوب می شوند [۱۰]. برای تضمین امنیت اطلاعات اقدامات لازم برای ارتقای آگاهی امنیتی کارکنان باید صورت گیرد [۳ و ۱۱-۱۳].

بنابراین، هدف این مقاله آن است که عوامل سازمانی و فردی که بر آگاهی از امنیت اطلاعات کارکنان اثرگذار بوده را شناسایی کرده و تأثیر آگاهی امنیتی کارکنان بر پیشگیری از حملات مهندسی اجتماعی را ارزیابی کند. بخش دوم کارهای مرتبط صورت‌گرفته و فرضیات موردنظر را ارائه کرده که به مدل تحقیق منجر خواهد شد. بخش سوم روش و نتایج پیمایش کمّی و ارزیابی از مدل تحقیق ارائه می‌کند. نتایج پیمایش در بخش چهارم مورد بحث قرار خواهد گرفت و بخش پنجم به نتیجه‌گیری خواهد پرداخت.

۲- مرور ادبیات تحقیق

تحلیل نظریات مورد استفاده در کارهای مشابه صورت‌گرفته نشان می‌دهد که نظریه عمل منطقی[2] و نظریه بسط‌یافته آن یعنی نظریه رفتار برنامه‌ریزی شده[3] در این مطالعات و تحقیقات مورد استفاده قرار گرفته است [۲ و ۱۴-۱۷]. نظریه عمل منطقی یک نظریه درون فردی است که مقاصد رفتاری و رفتار واقعی را پیش‌بینی می‌کند [۱۸]. نظریه رفتار برنامه‌ریزی شده معتقد است که مقاصد رفتاری شخص از طریق سه عامل مستقل تعیین می‌شود: ۱- نگرش نسبت به رفتار ۲- هنجار ذهنی و ۳- سطح کنترل رفتار ادراکی [۱۸]. در بطن سیاستهای امنیت اطلاعات، مقاصد[نیّات] رفتاری تعیین می‌کند که یک شخص چگونه خود را با سیاست‌های امنیت اطلاعات سازمان تطبیق می‌دهد. عسکر و تمتام[4] [۴۱] معتقدند چهار عامل سیاست، رفتار کاربر، دانش نسبت به فناوری اطلاعات و آموزش در آگاهی از امنیت اطلاعات کارکنان موثرند. گولنکو[5] از نظریه رفتار برنامه‌ریزی شده به عنوان یک بنیان نظری برای توسعه اپلیکیشنی که موجب افزایش آگاهی مسائل امنیتی در فیس‌بوک شده استفاده می‌کند [۱۴]. روچا فلورس و اکستد[6] [۲] نشان دادند که رهبری تحولی[7] ، فرهنگ امنیت اطلاعات و میزان آگاهی عوامل تعیین کننده‌ای هستند که در پیشگیری از حملات مهندسی اجتماعی موثرند. ساریداکیس[8] و دیگران [۱۵] رفتار کاربرانی را که در سایتهای شبکه های اجتماعی تبدیل به قربانیان جرایم سایبری شده‌اند را بررسی کرده‌اند. سیپونن[9] و دیگران [۱۶] از یک مدل چند نظریه‌ای برای ارزیابی عوامل موثر بر رعایت سیاست‌های امنیت اطلاعات استفاده کرده‌اند.

نظریه رفتار برنامه‌ریزی شده به عنوان پایه نظری این تحقیق به خاطر کاربردپذیری آن با توجه به موضوع این تحقیق انتخاب گردید. از آنجایی که این تحقیق بر روی آگاهی از امنیت اطلاعات کارکنان متمرکز بوده، باید عوامل موثر بر مقاصد رفتاری کاربر برای پیشگیری از حملات مهندسی اجتماعی شناسایی شوند.

[1] Spearphishing

[2] Theory of reasoned action [TRA]
[3] Theory of planned behavior [TPB]
[4] Asker&Tamtam
[5] Gulenko
[6] Rocha Flores & Ekstedt
[7] Transformational leadership
[8] Saridakis
[9] Siponen

بدینسان ، بعد ابتکاری این تحقیق، توسعه یک مدل نواورانه است که در آن عوامل سازمانی و فردی مرتبط که بر آگاهی از امنیت اطلاعات و به تبع آن بر پیشگیری از حملات مهندسی اجتماعی موثر بوده با یکدیگر ترکیب شده‌اند. آگاهی امنیتی یا آگاهی از امنیت اطلاعات[1] به عنوان درک شخصی کارمند از دانش عمومی‌اش در مورد امنیت اطلاعات و آگاهی و درک او نسبت به سیاست‌های امنیت اطلاعات سازمانش تعریف می‌شود [۲ و ۱۹]. مراد از قصد یا نیّت ساختارمند ، قصد کارمند برای پیشگیری از حملات مهندسی اجتماعی است [۲]. در ذیل، چندین فرضیه که از تحقیقات صورت‌گرفته و مصاحبه با کارشناسان استخراج شده آورده شده است. جدول(۱) جمع‌بندی آنها را نشان می‌دهد.

تأثیر رهبری به عنوان یک عامل سازمانی که بر آگاهی از امنیت اطلاعات موثر است در تحقیقات صورت گرفته مورد بحث قرار گرفته است. در این تحقیقات، رهبری به عنوان اقدامات رهبر برای ایجاد آگاهی و انگیزه در کارکنان برای تغییر رفتارهای امنیت اطلاعاتشان به صورتی که تمامی کارکنان به راحتی و به روشنی اهداف سیاست‌ها و اقدامات امنیت اطلاعات سازمان را درک کنند تعریف شده است [۲]. یورینا کونولی[2] و دیگران معتقدند که به اشتراک‌گذاری ارزشهای مشترک و داشتن حس مسئولیت‌پذیری برای موفقیت سازمان‌شان حائز اهمیت است [۲۰]. روچا فلورس و اکستد نشان می‌دهند که رفتار مدیران امنیتی تاثیر مثبتی بر روی کارکنان دارد[۲]. بدینسان، فرضیه ۱ عنوان می‌کند که رهبری، تأثیر مثبتی بر روی آگاهی از امنیت اطلاعات کارکنان دارد.

امکان دیگر برای ارتقای آگاهی از امنیت اطلاعات و ترغیب کارکنان برای انجام اقدامات لازم در راستای منافع سازمان، اعلان سیاست‌های امنیت اطلاعات سازمان است. هدف این سیاست آن است که تمامی کارکنان بتوانند به راحتی هدف اقدامات انجام گرفته در راستای امنیت اطلاعات را در سازمان درک کنند [۲]. یورینا کونولی و دیگران دریافتند که ایجاد سیاست‌های امنیت اطلاعات به صورت غیرمستقیم از طریق آگاهی از امنیت اطلاعات بر روی اقدامات کارکنان تأثیرگذار است [۲۰]. این بدان معناست که آگاهی کارکنان از الزامات امنیت اطلاعات سازمانی، تهدیدات سازمانی و پیامدهای فعالیت‌های غیرقانونی می‌تواند باعث افزایش رفتارهای سازگارپذیر کارکنان شود که این کار به فرضیه دوم ختم می‌شود.

جدول(۱): فرضیات

شماره	فرضیه	مرجع
۱	رهبری تأثیر مثبتی بر آگاهی از امنیت اطلاعات دارد.	[۲۰]
۲	سیاست‌های امنیتی تأثیر مثبتی بر آگاهی از امنیت اطلاعات کارکنان دارد.	[۲۰]
۳	برنامه‌های آگاه‌سازی و آموزش و مهارت‌آموزی امنیتی[3] تأثیر مثبتی بر آگاهی از امنیت اطلاعات کارکنان دارد.	[۲۲-۲۵]
۴	اعتماد بیش از حد[اعتماد بی‌جا] رابطه معکوسی با آگاهی از امنیت اطلاعات کارکنان دارد.	[۲۵-۲۷]
۵	ریسک‌کردن کمتر با آگاهی از امنیت اطلاعات کارکنان رابطه مستقیمی دارد.	[۲۹]
۶	آگاهی از امنیت اطلاعات کارکنان تأثیر مثبتی بر بینش آنها نسبت به پیشگیری از حملات مهندسی اجتماعی دارد.	[۱۴]
۷	آگاهی از امنیت اطلاعات کارکنان رابطه مستقیمی با کنترل رفتار ادراکی دارد.	[۱۴]
۸	آگاهی از امنیت اطلاعات کارکنان رابطه مستقیمی با هنجار ذهنی ادراکی دارد.	[۱۴]
۹	آگاهی از امنیت اطلاعات کارکنان رابطه مستقیمی باانگیزه آنان در مقابله با مهندسی اجتماعی دارد.	[۱۸و۲۹]
۱۰	بینش کارکنان رابطه مستقیمی باانگیزه آنها برای مقابله با مهندسی اجتماعی دارد.	[۱۴و ۱۶و ۲۲و ۲۷و ۳۰]
۱۱	کنترل رفتاری ادراکی کارکنان رابطه مستقیمی باانگیزه آنها برای مقابله با حملات مهندسی اجتماعی دارد.	[۱۴و ۱۶و ۲۲و ۲۷و ۳۰]
۱۲	هنجار ذهنی کارکنان رابطه مستقیمی باانگیزه آنها برای مقابله با حملات مهندسی اجتماعی دارد.	[۱۴و ۱۶و ۲۲و ۲۷و ۳۰]

دارسی[4] و دیگران معتقدند که برنامه‌های آگاه‌سازی، آموزش و مهارت‌آموزی امنیتی برای پیشگیری از سوء استفاده از سیستم های اطلاعات ضروری هستند [۲۱]. اسمیت[5] و دیگران توضیح

[1] Information security awareness [ISA]
[2] Yuryna Connolly
[3] Security education, training and awareness programs [“SETA programs”)
[4] Darcy
[5] Smith

می دهند که این روش دفاعی نه تنها کاربران را در مورد نتایج حملاتی که شناسایی شده‌اند آگاه می‌کند بلکه همچنین به توسعه درک عمیق‌تر از اصول اساسی آن کمک می‌کند. کارمندان در صورتی که قادر به شناخت ویژگی‌های خاص حملات باشند، احتمال بیشتری دارد که تهدیدات را شناسایی کنند [۱۳]. تحقیقات مرتبط دیگر نیز نتیجه گرفتند که یکی از راه‌های موثر برای پیشگیری از حملات مهندسی اجتماعی آموزش کارکنان است [۲۲-۲۵]. این یافته‌ها منجر به شکل گیری فرضیه سوم شد.

همان‌طور که قبلاً عنوان شد، عوامل فردی نیز بر روی آگاهی از امنیت اطلاعات کارکنان اثرگذار است. وورکمن[1] [۲۶] در مورد رویکرد حملات مهندسی اجتماعی بحث می‌کندکه در آن یک قربانی بالقوه برای همراهی با مهاجم و برای اعتماد به او از طریق ایجاد یک رابطه انتخاب می‌شود. مهندسان اجتماعی از الگوی اعتماد از طریق سوء استفاده از نیاز فرد به رابطه دوستانه، ایجاد شبیه‌سازی با قربانی احتمالی، جعل ارتباطات شخصی یا حتی وانمود کردن یک شخص مشهور استفاده می‌کنند. زبان و دانش شواهد وضعیتی موجب ایجاد اعتبار و اعتماد برای فریب قربانیان احتمالی می‌شود [۲۷]. اعتماد به محیط برخط می‌تواند به عنوان تمایل به اتکا به دیگران برای انجام تعهدات و قول‌های آنها دیده شود؛ باوری که دیگران از اطلاعات شخصی به شیوه‌ای اخلاقی استفاده کرده یا این تصور که هرگونه ارتباط با طرف دیگر ارتباط امنی است [۲۵]. یورینا کونولی و دیگران [۲۰] همچنین به موضوع اعتماد در حوزه امنیت اطلاعات سازمان پرداخته‌اند. آنها معتقدند که درجه بالایی از سازگاری اجتماعی منجر به ایجاد یک تعهد یا قرارداد خاص میان کارکنان شده که به موجب آن به یکدیگر اعتماد می‌کنند که این موضوع به فرضیه چهارم منتج می‌شود.

اعتماد ارتباط تنگاتنگی با مفهوم خطر(ریسک) دارد [۲۸]. بنابراین، عامل فردی دوم مورد توجه این تحقیق تمایل یک کارمند به خطر کردن است. خطر درک شده[ادراکی] عاملی است که به پیش بینی احتمال پذیرش ریسک[خطر کردن] توسط فرد در یک شرایط نامعین کمک می‌کند [۲۵]. هرچند پذیرش خطر در شرایط مختلف متفاوت است اما تمایل به پذیرش خطر تقریباً ثابت است. در محیط سازمانی، کارکنان خطرهایی را می پذیرند مثل ارتباط برقرارکردن با افراد غریبه به صورت برخط یا به اشتراک‌گذاری اطلاعات شخصی که می‌تواند احتمال حملات مهندسی اجتماعی را افزایش دهد [۱۵]. ثابت شده که بر حسب شخصیت، افراد وظیفه‌شناس‌تر، هم سازتر و انعطاف‌پذیرتر و کسانی که تمایل کمتری به پذیرش خطر دارند آگاهی امنیت اطلاعات بالاتری دارند [۲۹]. بنابراین فرضیه پنجم شکل می‌گیرد.

تأثیر آگاهی از امنیت اطلاعات به عنوان یک عامل مرکزی امنیت اطلاعات دیده شده است [۲۹ و ۳۰]. هدف از ایجاد این نوع آگاهی توانمندسازی کارکنان در خصوص خطرات امنیت اطلاعات و آموزش آنها در مورد نقش‌ها و مسئولیت‌پذیری‌هایشان است. بر اساس نظریه رفتار برنامه‌ریزی شده [۱۸]، آگاهی از امنیت اطلاعات نه تنها بر عقاید کارکنان در مورد نتایج و پیامدهای کار تاثیرگذار است، بلکه همچنین تاثیر مستقیمی بر تمایل فرد به پذیرش امنیت اطلاعات دارد [۱۹]. مراد از تمایل در اینجا به عنوان میزانی که در آن عملکرد رفتار امنیت اطلاعات ارزش‌گذاری شده تعریف شده است [۲]. به‌علاوه، نشان داده شد که افزایش آگاهی از امنیت اطلاعات تاثیر مثبتی بر گرایش فرد داشته و به کارمندان در درک بهتر اهمیت اقدامات انجام شده در راستای حفظ امنیت اطلاعات کمک می‌کند [۲۰]. به‌علاوه، با توجه به کنترل رفتار ادراکی، آگاهی از تهدیدات امنیت اطلاعات برای شناسایی روشهای معمول مهندسی اجتماعی و واکنش نسبت به آن برای کارکنان حیاتی است [۲]. مراد از کنترل رفتاری ادراکی در اینجا میزان کنترلی است که شخص فکر می‌کند که در برابر حملات مهندسی اجتماعی دارد. گولنکو [۱۴] همچنین بیان می‌کند که آگاهی از امنیت اطلاعات یک عامل حیاتی در افزایش کنترل رفتاری ادراکی کارکنان است. به‌علاوه، تأثیر هنجارهای ذهنی بر روی رفتار در مطالعات انجام شده مورد بحث قرار گرفته است. بدینسان ، افراد رفتارشان را به سمت رفتار چرخه اجتماعی‌شان تنظیم می‌کنند [۲]. طبق این گفته، فرد در زمانی که محیط اجتماعی تغییر می‌کند، هوشیارانه‌تر رفتار می‌کند [۱۴]. طبق تحقیق مذکور، فرضیات شش، هفت و هشت در نظر گرفته شده‌اند.

به‌علاوه، یورینا کونولی و دیگران [۲۰] معتقدند که آگاهی از امنیت اطلاعات یک عامل مهم در ترغیب رفتار پذیرا [مطیع] است. نتایج مطالعه آنها نشان می‌دهد که کارمندان هنگامی که می‌فهمند که علّتی برای مقررات خاص وجود دارد، تمایل بیشتری برای به‌کاربستن اقدامات امنیتی دارند. مک کورماک و دیگران نشان می‌دهند که دانش تهدیدات احتمالی و اقدامات حفاظتی نه تنها بر نگرش افراد تأثیرگذار است بلکه منجر به رفتار پذیرنده می‌شود [۲۹]. همان‌طور که جمع‌آوری داده‌ها روی رفتارهای واقعی به ویژه در حوزه امنیت اطلاعات، چالش برانگیز است [۲] و طبق نظریه رفتار برنامه‌ریزی‌شده، مقصود[انگیزه] پیش نیاز آنی رفتار واقعی است [۱۸] و این مطالعه بر روی اخذ نیّات کارکنان متمرکز بوده و از این نظر فرضیه نهم مطرح می‌شود.

[1] Workman

عامل اصلی نظریه رفتار برنامه‌ریزی شده مقصود [نیت] یک فرد برای انجام یک رفتار است [۱۸]. هرچقدر نیّت فرد در مسیر رفتار واقعی باشد، احتمال بیشتری دارد که آن رفتار انجام شود.تغییرات صورت گرفته در نیّت از طریق بینش، کنترل رفتار ادراکی و هنجارهای ذهنی توضیح داده شده‌اند. روچا فلورز و اکستد دریافتند که این سه عامل درونی مستقیماً بر انگیزه و نیّت افراد برای مقابله با حملات مهندسی اجتماعی موثرند [۲]. سیپونن و دیگران همچنین تاثیرمثبت این سه عامل در نیت کارکنان برای همراهی با سیاستهای امنیت اطلاعات را نشان داده‌اند [۱۶]. کارهای قبلی دیگر انجام شده [مثل۱۴, ۲۲، ۲۷ و ۳۰] نیز از فرضیات دهم، یازدهم و دوازدهم حمایت می‌کنند.

در خصوص پیشینه این موضوع در داخل کشور نیز می‌توان گفت در خصوص موضوع موردنظر هیچ‌گونه تحقیقی صورت نگرفته لیکن در خصوص موضوع آگاهی از امنیت اطلاعات کاربران و کارکنان تحقیقات بسیار محدودی صورت‌گرفته که از آن جمله می‌توان به مقاله پیکری و بنازاده [۳۷]اشاره کرد که نتیجه کار ایشان نشان می‌دهد آگاهی از امنیت اطلاعات با هنجارهای فردی، خودکنترلی و قصد نقض امنیت اطلاعات رابطه معناداری داشته و نیز هنجارهای فردی و خودکنترلی با قصد نقض امنیت اطلاعات رابطه معنادار دارند.

تحقیق دیگر توسط حسن‌زاده و دیگران [۳۸]انجام شده که نشان می‌دهد داشتن مهارت فناوری اطلاعات، درجه سازمانی، رشته تحصیلی و رده شغلی کارکنان بر پرمایگی آگاهی ایشان از امنیت اطلاعات همبستگی دارد و ضرورت آموزش امنیت اطلاعات اثبات شده و در برنامه‌ریزی آموزش امنیت اطلاعات بایستی درجه سازمانی، رشته تحصیلی و رده شغلی مورد توجه قرار گیرد.

۳. مطالعه تجربی

بر اساس فرضیات مطرح شده، این فصل به مطالعه تجربی انجام شده پرداخته و طراحی تحقیق و انجام پیمایش شرح داده می‌شود. سپس داده‌های جمع‌آوری شده ارائه شده و نتایج تحلیل می‌شوند.

۳-۱ طراحی پرسش‌نامه و جمع‌آوری داده‌ها

جمع‌آوری صورت گرفته از طریق مطالعات و تحقیقات صورت گرفته و مرور ادبیات مطرح شده در بخش قبلی و نیز مصاحبه با ۱۶ نفر از کارشناسان حوزه مهندسی اجتماعی، مورد تحلیل قرار گرفت و گزاره‌های مورد نظر به دست آمد. سوالات با توجه به هدف این تحقیق تهیه و تنظیم شدند که مسائلی مثل رهبری[۲]، آموزش امنیت اطلاعات[۲۱]، برنامه آگاه‌سازی، آموزش و مهارت‌آموزی امنیتی[۲۱]، اعتماد[۲۵ و ۲۶]، ریسک[۱۵ و ۲۸]، آگاهی از امنیت اطلاعات[۲ و ۱۹]، بینش[۲]، کنترل رفتار ادراکی [۲، ۱۵ و ۲۶]، هنجار ذهنی [۲]، قصد و نیت [۲ و ۱۹]، در آن گنجانده شدند. برای پاسخ به پرسش‌نامه طراحی شده، از طیف ۵ نمره‌ای لیکرت[کاملاً موافق، تا حدی‌موافق، بی‌طرف، تا حدی مخالف و کاملاً مخالف] استفاده گردید. به‌علاوه، این پرسشنامه حاوی سوالات جمعیت‌شناختی نیز بود از قبیل جنس، سن تولد، شغل و ...]. این تحقیق نوعی تحقیق اکتشافی نیز محسوب شده چرا که در تحقیقات قبلی تمامی عوامل سازمانی و فردی موثر بر آگاهی از امنیت اطلاعات کارکنان در یک تحقیق واحد مطرح نشده است.

در روایی و پایایی مصاحبه از روش لینکلن و گویا[1] استفاده شد که چهار معیار اعتبارپذیری، ثبات‌پذیری، تأییدپذیری و انتقال‌پذیری مدّنظر قرار گرفت. در بخش اعتبارپذیری مشارکت‌کنندگان با حداکثر تنوع تجربیات و تخصص انتخاب شدند و نمونه‌گیری تا رسیدن نمونه به حد اشباع ادامه یافت. برای ثبات‌پذیری از یک ناظر خارجی برای افزایش میزان ثبات پژوهش استفاده گردید و از طولانی‌شدن زمان جمع‌آوری داده‌ها خودداری گردید. سازگاری مطالب حاصله با نوشته‌ها و تحقیقات قبلی نشان‌دهنده تأییدپذیری تحقیق بوده و نیز بخشی از مطالب ارائه شده تجارب واقعی افراد مشارکت‌کننده بوده است. در خصوص انتقال‌پذیری نیز طبق نظر لین کولن و گویا این بخش از تحقیق در مرحله کیفی وظیفه محقق نبوده چرا که به دنبال تعمیم‌دادن نتایج آن نبوده است.

برای ارزیابی پرسش‌نامه نیز از لحاظ جامعیت و صحت ساختاری، یک پیش‌آزمون انجام شد که در آن ۱۹ نفر از افرادی با سن و جایگاه‌های شغلی مختلف در شهرداری تهران حضور داشتند. از پاسخ دهندگان پیش‌آزمون خواسته شد تا در مورد هر سوال نظراتشان را ارائه دهند. بر اساس نظرات ایشان و نتایج پیش‌آزمون، جمله‌بندی و سازماندهی سوالات تا حدودی بازنگری گردید.

بخشی از این پرسش‌نامه‌ها به‌صورت حضوری و در فرم‌های کاغذی و بخشی دیگر به دلیل عدم دسترسی به‌تمامی کارکنان[پراکندگی جغرافیایی، محدودیت‌های کرونایی و...] از طریق فضای مجازی[ایمیل و شبکه‌های اجتماعی] ارسال گردید. در مجموع ۱۳۶۲ نفر از کارمندان مناطق ۲۲ گانه تهران در این پیمایش شرکت کردند. سپس داده‌های جمع‌آوری شده از لحاظ کامل‌بودن و متناسب بودن پاسخ‌ها ارزیابی گردید. باتوجه‌به ارزیابی انجام شده ۴۰ مورد از پرسش‌نامه‌های پاسخ داده شده حذف گردید که مشخص بود به‌درستی پرسش‌نامه را تکمیل

[1] Lincoln&Guba

نکرده یا پاسخ‌های آنها معتبر نیست. در نهایت تعداد ۱۳۲۲ پرسش‌نامه صحیح و کامل برای تحلیل داده‌ها مورداستفاده قرار گرفت.

۳-۲- ویژگی‌های نمونه:

دسته‌بندی جنسیتی نشان می‌دهد که تعداد مردان بیش از زنان بوده به‌طوری‌که بیش از ۷۰ درصد جمعیت نمونه را به خود اختصاص داده‌اند که در مجموع ۹۶۵ نفر مرد و ۳۵۷ نفر زن بودند. هرچند ممکن است این تفاوت آماری در تعداد زن و مرد موجب جهت‌گیری در نتایج شود؛ اما بررسی‌های آتی نشان خواهد داد که تفاوت جنسیتی نقش چندانی را ایفا نمی‌کند. توزیع سنّی پاسخ‌دهندگان نیز نشان‌دهنده آن است که اکثر شرکت‌کنندگان بین ۳۰ تا ۴۰ سال و در مرتبه بعدی بین ۴۰ تا ۵۰ سال سن داشته‌اند. قریب به‌اتفاق شرکت‌کنندگان متأهل بوده و حدود ۲۴ درصد آنها مجرد بودند. میزان تحصیلات شرکت‌کنندگان نیز نشان‌دهنده آن است که اکثر آنها دارای مدرک لیسانس بودند. در مورد شغل نیز توزیع کمّی مناسبی میان شرکت‌کنندگان از نظر نوع شغل وجود داشته و پراکندگی شرکت‌کنندگان در حدّ مناسبی بوده است؛ بااین‌وجود تعداد افرادی که در بخش ترافیک و حمل‌ونقل مشغول به کار بودند بیش از دیگران بوده است. جدول(۲) مشخصات جمعیت‌شناختی شرکت‌کنندگان را نشان می‌دهد:

جدول(۲): مشخصات جمعیت‌شناختی شرکت‌کنندگان

متغیر	فراوانی	درصد
جنسیت		
مرد	۹۶۵	۷۳
زن	۳۵۷	۲۷
سن		
زیر سی‌سال	۱۸۸	۱۴,۲۲

۳-۳- ارزیابی پیمایش

برای ارزیابی مدل ساختاری و نیز ارزیابی فرضیه‌ها، روش مدل‌سازی معادلات ساختاری با حداقل مربعات جزئی[1] انتخاب گردید. این روش یک روش مدل سازی علّی است که هدفش حداکثرسازی انحراف معیار سازه‌های پنهان وابسته است [۳۱ و ۳۲]. PLS-SEM انحراف‌محور مورد استفاده قرار گرفت چرا که برای جمعیت‌های نمونه کوچک و نه چندان بزرگ مناسب است [۳۱ و ۳۲]. در گام اول ، قبل از اینکه ضریب مسیر[2] برای مدل ساختاری محاسبه شود[3]، مدل سنجش ارزیابی و مورد بازنگری قرار گرفت. جزئیات این مراحل در جدول (۳) ارائه شده است.

جدول(۳): تعداد نهایی گزاره‌های هر سازه، محدوده بار عاملی[4]، آلفای کرونباخ[5]، پایایی ترکیبی[6] و میانگین واریانس استخراج شده[7]

سازه	تعداد گزاره‌ها	بار عاملی: حداقل	بار عاملی: حداکثر	آلفای کرونباخ	پایایی ترکیبی	میانگین واریانس استخراج شده
بینش	۴	۰,۶۴۵	۰,۷۳۸	۰,۷۶۱	۰,۸۳۶	۰,۶۰۵
مقصود [نیّت]	۵	۰,۶۳۸	۰,۸۵۹	۰,۶۹۳	۰,۸۸۵	۰,۶۸۳
آگاهی از امنیت اطلاعات	۶	۰,۶۸۰	۰,۸۴۰	۰,۷۶۸	۰,۸۲۹	۰,۵۸۵
سیاست گذاری امنیت اطلاعات	۵	۰,۸۴۹	۰,۶۴۵	۰,۷۸۳	۰,۸۷۴	۰,۵۸۰
رهبری	۶	۰,۶۸۳	۰,۸۹۳	۰,۸۶۴	۰,۹۶۳	۰,۶۵۹
کنترل رفتاری ادراکی	۴	۰,۶۸۴	۰,۷۹۳	۰,۸۱۹	۰,۸۴۲	۰,۵۴۷
ریسک	۵	۰,۸۹۳	۰,۸۶۲	۰,۵۳۹	۰,۸۴۹	۰,۵۴۸
برنامه آگاهسازی آموزش و مهارت‌آموزی امنیتی	۶	۰,۸۷۵	۰,۷۳۹	۰,۸۶۴	۰,۹۲۷	۰,۶۴۲
هنجار ذهنی	۳	۰,۷۵۳	۰,۶۹۳	۰,۷۸۴	۰,۸۹۵	۰,۸۷۴
اعتماد	۵	۰,۸۰۳	۰,۷۹۶	۰,۸۴۹	۰,۹۳۷	۰,۶۴۸

[1] PLS-SEM

[2] Path coefficients

[3] ضریب مسیر بیان کننده رابطه علّی خطی و شدت و جهت این رابطه بین دو متغیر است. در واقع همان ضریب رگرسیون در حالت استاندارد است که در مدل‌های ساده‌تر رگرسیون ساده و چندگانه مشاهده می‌شود. عددی بین ۱- و ۱+ که اگر برابر صفر باشد نشان‌دهنده نبود رابطه علّی خطی بین دو متغیر پنهان است.

[4] Factor loading limits

[5] Cronbach's alpha

[6] Composite Reliability

[7] Average Variance Extracted

یک مدل سنجش بازتابی با استفاده از اسمارت پی ال اس[1] مدل‌سازی شد؛ همچنان که شاخص‌های سازه‌های پنهان به عنوان معلول آن عامل[یعنی سازه] در نظر گرفته شده‌اند [۳۴ و ۳۵]. برای ارزیابی مدل بیرون، در ابتدا همگرایی و بارگیری عاملی در نظر گرفته شدند. تحلیل بارگیری عاملی در سطح شاخص اطلاعاتی را در مورد میزان تناسب شاخص ها برای مقیاس سازه پنهان ارائه می‌دهد [۳۳]. مقدار یا ارزش بالاتر یا نزدیک به ۰,۷ برای پایایی شاخص قابل قبول است [۳۱]. از نتایج حاصل از اولین ارزیابی چندین گزاره کنار گذاشته شدند چرا که مقادیر آنها زیر آستانه مورد نظر بود. به‌علاوه، بارگیری‌های توزیعی مدّنظر قرار گرفت و دو گزاره دیگر نیز حذف شدند چرا که شبیه سازه‌های دیگری بودند که ارزش آنها بالای ۰,۶ بود. از طرف دیگر، عوامل[فاکتورها] با مقادیر بالای ۰,۶ برای تحلیل حفظ شدند چرا که آنها بارگیری عرضی با دیگر سازه‌ها نداشتند. با این تطبیق، همگرایی در هشت دور تکرار حاصل گردید. شمایی کلی از تعداد باقی مانده گزاره‌ها و محدوده بارگیری عامل [یعنی حداقل و حداکثر مقدار بارگیری عامل گزاره‌ها] در جدول ۳ ارائه شده است.

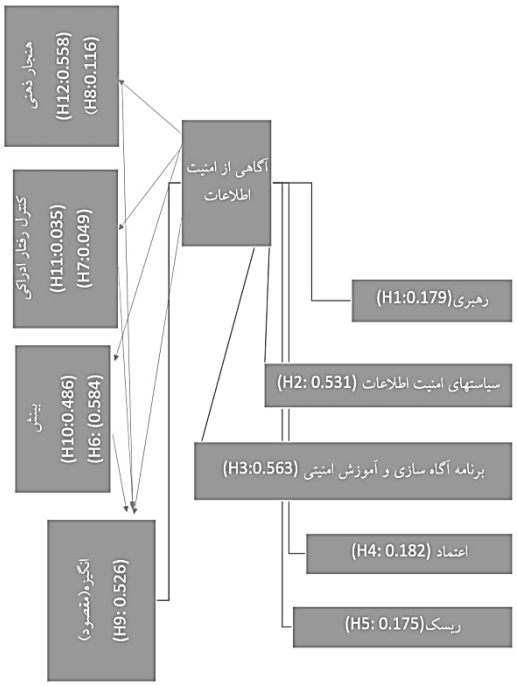
سپس پایایی و روایی سازه‌ها مورد ارزیابی قرار گرفتند. جدول ۳ همچنین حاوی نتایج آلفای کرونباخ، پایایی ترکیبی و میانگین واریانس استخراج شده است. آلفای کرونباخ نشان می‌دهد که آیا شاخص‌های متغیر پنهان دارای روایی همگرا بوده و آیا پاسخ‌های بین گزاره‌ها هم‌خوانی دارد یا خیر و بنابراین قابلیت اعتماد را نشان می‌دهند [۳۶]. از آنجایی که آلفای کرونباخ می‌تواند قابلیت اعتماد یا اعتبار یک مقیاس را تخمین بزند، پایایی ترکیبی معمولاً به عنوان جایگزینی برای آزمایش روایی همگرا مورد استفاده قرار می‌گیرد و براساس هماهنگی درونی سوالات هر عامل محاسبه می‌شود بنابراین معیار دقیق‌تری است. در مطالعات اکتشافی، مقادیر بالای ۰,۶ برای پایایی ترکیبی قابل قبول در نظر گرفته می‌شوند [۳۱]. روایی همگرا با شاخص میانگین واریانس استخراج شده محاسبه می‌شود و نشان می‌دهد چقدر گویه‌های یک سازه باهم ارتباط و انطباق درونی دارند. میانگین واریانس استخراج شده، درصد انحراف به دست آمده از طریق یک سازه را نشان می‌دهد[۳۵] در یک مدل مناسب، عوامل[فاکتورها] باید حداقلی نیمی از انحراف شاخص‌های نسبی‌شان را توضیح دهند[یعنی میانگین واریانس استخراج شده باید بالای ۰,۵ باشد] [۳۶]. همان‌طور که در جدول ۳ نشان داده شده، مقادیر آلفای کرونباخ برای رفتار خطرناک[دارای ریسک] زیر محدوده پیشنهادی ۰,۶ برای مطالعات اکتشافی است. هرچند از آنجایی که مقادیر پایایی ترکیبی و میانگین واریانس استخراج شده بالای آستانه هستند، رفتار خطرناک[ریسک] نیز در تحلیل داده‌ها مدّنظر قرار گرفته است.

مدل درونی ابتدا از طریق روش بلایندفولدینگ[2] و تحلیل مقدار Q^2 استون-گیسر[3] ارزیابی گردید. مقادیر Q^2 بین 0.1 و ۰,۱۹ [یعنی همگی بالای صفر] بودند که پایایی پیشگوی[4] مدل ساختاری را تأیید می‌کند[۳۶]. سپس این مدل از طریق بوت استرپینگ[5] چک گردید تا معنادار بودن ضریب مسیر را ارزیابی کند. سطح معناداری ۰,۱ برای زیرنمونه ها در نظر گرفته شد. مقادیر t بحرانی برای آزمایش دو مرحله ای ۱,۸۳ بود[سطح معناداری $p < 10\%$] ، ۱,۷۸[$p < 5\%$] و ۱,۳۷[$p < 1\%$] . اندازه اثر برای تعیین اثر بر روی متغیر پنهان درون‌زا مورد استفاده قرار می گیرد. مقدار بالای ۰,۳۵، ۰,۱۵ و ۰,۰۲ به ترتیب بالا، متوسط و پایین در نظر گرفته شده‌اند [۳۳]. ضریب مسیر نشان‌دهنده شدت رابطه میان متغیرهای پنهان است. مسیرهایی که هیچ گونه رابطه ای با مسیر فرضی نداشته، از فرضیات در نظر گرفته شده حمایت نمی‌کنند. چنین مقادیری منجر به ردّ فرضیات مربوطه می‌شود.

در ارزیابی نهایی مدل ساختاری علاوه بر ضریب‌های مسیر و سطح معناداری، میزان واریانس تشریح شده [R^2] لحاظ شده است. بر اساس ضرایب مسیر معنادار و نتایج به‌دست‌آمده، فرضیات دوم، سوم، نهم، دهم و دوازدهم کاملاً تأیید [$p < 0.01$] ، فرضیات اول و چهارم و پنجم حمایت ضعیفی شدند [$p < 0.1$] و فرضیات هفتم، هشتم و یازدهم رد شدند. شکل(۱) شمایی کلی از مدل ساختاری و سطح معناداری هر کدام از فرضیه‌ها را نشان می‌دهد.

[1] SmartPLS

[2] Blindfolding
[3] Stone-Geisser's Q^2
[4] Predictive relevance
[5] Bootstrapping



شکل(۱): ضریب‌های مسیر و سطح معناداری مدل ساختاری تحقیق

۴- یافته‌های تحقیق:

یافته‌های تحقیق نشان می‌دهد که آگاهی از امنیت اطلاعات از منظر کارکنان شهرداری تهران، تحت‌تأثیر رفتارهای پرمخاطره است؛ اما شدت آن ضعیف است. هرچند مطالعات قبلی صورت‌گرفته ریسک را به‌عنوان یک عامل شخصی مرتبط با آگاهی از امنیت اطلاعات در نظر گرفته‌اند؛ اما هیچ‌کدام از آنها تأثیر قوی این عامل را نشان نمی‌دهند. برخلاف تحقیق مک‌کورماک۱ و دیگران [۲۹] که نشان می‌دهد که افراد روشن‌فکر، دلسوز و وظیفه‌شناس و افرادی که تمایل به ریسک‌کردنشان پایین است دارای آگاهی از امنیت اطلاعات بالایی هستند، این تحقیق ضمن تأیید مؤثربودن آن اما میزان آن را در میان کارکنان شهرداری تهران ضعیف می‌داند. این موضوع در خصوص عامل فردی دوم؛ یعنی اعتماد نیز صادق است.

از سه عامل سازمانی موثر بر آگاهی از امنیت اطلاعات، سیاستهای امنیت اطلاعات و برنامه‌های آگاه‌سازی، آموزش و مهارت‌افزایی امنیتی رابطه محکمی با آگاهی از امنیت اطلاعات داشته و رهبری رابطه ضعیفی در این بین دارد. همانند تحقیقات دیگر صورت گرفته [۲۰ و ۲۱]، نتایج این تحقیق نیز نشان می‌دهد که رابطه معناداری میان سیاستهای امنیتی و آگاهی از امنیت اطلاعات وجود دارد. همین موضوع در خصوص رابطه میان برنامه‌های آگاه‌سازی، آموزش و مهارت‌افزایی امنیتی و آگاهی از امنیت اطلاعات نیز صدق می‌کند. روچا فلورس و اکستد همبستگی معناداری را میان رهبری و اگاهی از امنیت اطلاعات یافتند [۲]. مطالعه آنها بر روی رابطه میان رهبری و مشارکت کارکنان در پیشگیری از حملات مهندسی اجتماعی متمرکز بود اما تنها آن را از طریق فرهنگ امنیت اطلاعات تشریح کرده‌اند. لذا اگر موضوع فرهنگ امنیت اطلاعات در سازمان را طبق نظریه فوق به رهبری پیوند دهیم، در آن صورت یافته‌های این تحقیق نشان می‌دهد که رابطه معنادار قوی میان فرهنگ امنیت اطلاعات در سازمان با آگاهی از امنیت اطلاعات وجود ندارد.

در خصوص ارزیابی تأثیر آگاهی از امنیت اطلاعات در این تحقیق، یافته‌ها نشان می‌دهد که آگاهی از امنیت اطلاعات تأثیر مستقیمی بر بینش‌های افراد نسبت به پیشگیری از مهندسی اجتماعی و نیز انگیزه و نیّت آنها برای مقابله با مهندسی اجتماعی دارد؛ اما در خصوص تأثیر آن بر کنترل رفتار ادراکی و هنجار ذهنی این موضوع صدق نمی‌کند.

بنابراین، این تحقیق نتایج مطالعات دیگر همچون روچا فلورس و اکستد [۲] و نیز نظریه رفتار برنامه‌ریزی شده که به بینش، کنترل رفتار ادراکی و هنجار ذهنی توجه داشتند می‌پردازند؛ تنها عامل بینش را در میان کارکنان شهرداری تهران مؤثر می‌داند. بنابراین طبق نتیجه تحقیق آگاهی از امنیت اطلاعات بر روی بینش افراد نسبت به پیشگیری از حملات مهندسی اجتماعی مؤثر بوده و کنترل رفتار ادراکی و هنجار ذهنی تأثیر چندانی ندارد.

علاوه براین، یک رابطه قوی میان بینش و انگیزه[نیّت] مقابله با مهندسی اجتماعی وجود دارد. این موضوع در دیگر تحقیقات انجام شده از جمله بولگورسو۲ و دیگران [۱۹]، یورینا کونولی و دیگران [۲۰] و دارسی و دیگران [۲۱] و روچا فلورس و اکستد[۲] نیز تأیید شده است. به‌علاوه هنجار ذهنی نیز بر انگیزه افراد برای مقابله با مهندسی اجتماعی موثر بوده اما کنترل رفتار ادارکی تأثیر چندانی ندارد.

۵- نتیجه‌گیری

این مطالعه بر روی نقش آگاهی از امنیت اطلاعات کارکنان و انگیزه و قصد آنها برای مقابله با حملات مهندسی اجتماعی متمرکز است. از دیدگاه نظری، نتایج به‌دست‌آمده کاربردپذیری نظریه رفتار برنامه‌ریزی شده در حوزه مهندسی اجتماعی را نشان می‌دهد هرچند برخی از مؤلفه‌های آن تأثیر چندانی در این تحقیق نداشتند. این نتایج همچنین نشان داد که سازمان‌ها باید درک کنند که انجام اقدامات فنی به‌تنهایی برای تضمین امنیت

[1] McCormac

[2] Bulgurcu

اطلاعات کافی نیست هرچند بسیار حائز اهمیت است. از دیدگاه مدیریتی، ارتقای سطح آگاهی کارکنان از اهمیت امنیت اطلاعات باید در رأس توسعه اقدامات انجام شده در راستای امنیت اطلاعات باشد. بنابراین، ارزیابی رفتارها خطرناک کارکنان، آموزش و برگزاری کارگاه‌هایی برای افزایش آگاهی و هشیاری کارکنان برای سازمان‌ها در پیشگیری از حملات مهندسی اجتماعی پیشنهاد می‌شود. بیشترین اقدامات تأثیرگذار طبق نتایج به‌دست‌آمده تدوین سیاست‌های امنیت اطلاعات، ایجاد برنامه‌های آگاه‌سازی و آموزش امنیتی، افزایش آگاهی از امنیت اطلاعات برای ایجاد بینش و انگیزه در کارکنان برای مقابله با مهندسی اجتماعی و نیز ایجاد هنجار ذهنی است.

هرچند انجام تحقیقات در خصوص عوامل انسان‌محور مهندسی اجتماعی امری لازم بوده؛ اما تحقیقات دیگری که در آنها به نقش فناوری و محیط در پیشگیری از حملات مهندسی اجتماعی پرداخته نیز ضروری به نظر می‌رسد. بنابراین انجام تحقیقاتی در خصوص ارزیابی انگیزه‌ها و علل درونی و بیرونی مهندسی اجتماعی می‌تواند به پیشگیری از مهندسی اجتماعی و کاهش اثرات آن کمک نماید.

انجام این تحقیق با محدودیت‌هایی نیز مواجه بوده است که از آن جمله می‌توان به نمونه نسبتاً کوچک تعداد افراد شرکت‌کننده اشاره کرد. بنابراین انجام پیمایش‌های دیگری با نمونه‌های بزرگ‌تر و در گروه‌های هدف خاص مفید خواهد بود و امکان مقایسه عوامل مؤثر را در میان کشورها، سازمان‌ها و صنایع مختلف و نیز کارکنانی که در جایگاه‌های شغلی مختلف مشغول به کار بوده را می‌دهد. محدودیت دیگر این تحقیق استفاده از نیّت و انگیزه افراد به‌جای سنجش رفتار واقعی آنهاست. قطعاً سنجش رفتار واقعی افراد می‌تواند نتایج دیگری را نسبت به سنجش انگیزه‌ها، تمایلات و نظرات ارائه دهد. هرچند تحقیقات و مطالعات قبلی صورت‌گرفته تأییدکننده این موضوع است که نیّت و انگیزه افراد، پیش‌بینی‌کننده رفتار واقعی آنها خواهد بود، اما هیچ تضمینی برای اینکه کارکنان همان‌طور که می‌گویند رفتار کنند وجود ندارد. بنابراین، مطالعات و تحقیقات دیگری باید انجام شود تا از یک گروه کنترل برای دست‌کاری عوامل خاص و سنجش رفتار واقعی کاربر استفاده کند

۶- مراجع

[1] Albladi SM, Weir GRS.ser characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, vol.8, No1 2018. https://doi.org/10.1186/s13673-018-0128-7.

[2] Rocha Flores W, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security, 59,pp.26-44, 2016. https://doi.org/10.1016/j.cose.2016.01.004.

[3] Stirnimann S. Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Wiesbaden: Springer Fachmedien Wiesbaden; 2018.

[4] Hauser D. Social Engineering Awareness in Business and Academia. In: MWAIS 2016 Proceedings; p.3, 2016.

[5] Bakhshi T. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In: 13th International Conference on Emerging Technologies [ICET]; 2017.

[6] Ivaturi K, Janczewski L. A Taxonomy for Social Engineering attacks. CONF-IRM 2011 Proceedings 2011.

[7] Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. Journal of Information Security and Applications vol.22, pp.22-113, ۲۰۱۵. https://doi.org/10.1016/j.jisa.2014.09.005.

[8] Ohaya C. Managing Phishing Threats in an Organization. In: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. New York, NY, USA: ACM, pp.159–161, 2006.

[9] Alazri AS. The awareness of social engineering in information revolution: Techniques and challenges. In: 10th International Conference for Internet Technology and Secured Transactions [ICITST]; pp.198–201, 2015.

[10] Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Computers & Education;vol.52[1], pp.92–100, 2009 https://doi.org/10.1016/j.compedu.2008.06.011.

[11] Mouton F, Leenen L, Malan MM, Venter HS. Towards an Ontological Model Defining the Social Engineering Domain. In: Kimppa K, Whitehouse D, Kuusela T, Phahlamohlaka J, editors. ICT and Society. Berlin, Heidelberg: Springer Berlin Heidelberg; pp.266–279. 2014

[12] Mouton F, Leenen L, Venter HS. Social engineering attack examples, templates and scenarios. Computers & Security, vol.59, pp.186–209. 2016 https://doi.org/10.1016/j.cose.2016.03.004.

[13] Smith A, Papadaki M, Furnell SM. Improving Awareness of Social Engineering Attacks. In: Dodge RC, Futcher L, editors. Information Assurance and Security Education and Training. Berlin, Heidelberg: Springer, pp. 249–256.2013

[14] Gulenko I. Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. Information Management & Computer Security; vol.21[2], pp.91–101. 2013 https://doi.org/10.1108/IMCS-09-2012-0053.

[15] Saridakis G, Benson V, Ezingeard J-N, Tennakoon H. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change;102, pp.320–30, 2016 https://doi.org/10.1016/j.techfore.2015.08.012.

[16] Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: An exploratory field study. Information & Management ;vol.51[2], pp.217–24. 2014. https://doi.org/10.1016/j.im.2013.08.006.

[17] Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior; vol.24[6], pp.2799–816. 2008 https://doi.org/10.1016/j.chb.2008.04.005.

[18] Ajzen I. The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes;50, pp.179–211. 1991

[19] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly;vol.34, No.3, pp.523–48. 2010

[20] Yuryna Connolly L, Lang M, Gathegi J, Tygar DJ. Organisational culture, procedural countermeasures, and employee security behaviour. Information and Computer Security;vol.25, No.2, pp.118–36, 2017. https://doi.org/10.1108/ICS-03-2017-0013.

[21] D'Arcy J, Hovav A, Galletta D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems

Research ;vol.20, No.1 ,pp.79–98, 2009 https://doi.org/10.1287/isre.1070.0160.
[22] Kruger H, Drevin L, Steyn T. A vocabulary test to assess information security awareness. Information Management & Computer Security;Vol.18, No.5, pp.316–27, 2010. https://doi.org/10.1108/09685221011095236.
[23] Vishwanath A, Herath T, Chen R, Wang J, Rao HR. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems;Vol.51, No.3, pp.576–86. 2011https://doi.org/10.1016/j.dss.2011.03.002.
[24] Wahyudiwan DDH, Sucahyo YG, Gandhi A. Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In: ICSITech: Proceedings 2017 3rd International Conference on Science in Information Technology "Theory and application of IT for education, industry, and society in big data era" October 25-26, 2017, Bandung, Indonesia. New York: IEEE;, pp. 654–658, 2018
[25] Wright RT, Marett K. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. Journal of Management Information Systems;Vol.27 No.1 ,pp.273–303. 2010. https://doi.org/10.2753/MIS0742-1222270111.
[26] Workman M. A test of interventions for security threats from social engineering. Information Management & Computer Security;Vol.16, No.5, ,pp.463–83. 2008. https://doi.org/10.1108/09685220810920549
[27] Stajano F, Wilson P. Understanding scam victims. Communications of the ACM;Vol.54, No.3, pp.70–5, 2011https://doi.org/10.1145/1897852.1897872.
[28] Öğütçü G, Testik ÖM, Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security; No.56 pp.83–93, 2016. https://doi.org/10.1016/j.cose.2015.10.002.
[29] McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, Pattinson M. Individual differences and Information Security Awareness. Computers in Human Behavior.No.69, pp.151–6, 2017. https://doi.org/10.1016/j.chb.2016.11.065.
[30] Mamonov S, Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior; No.83, pp.32–44, 2018. https://doi.org/10.1016/j.chb.2018.01.028.
[31] Hair JF, Ringle CM, Sarstedt M. PLS-SEM: Indeed a silver bullet. The Journal of Marketing Theory and Practice, Vol.19, No.2. pp.139–52, 2011
[32] Hair JF. A primer on partial least squares structural equations modeling [PLS-SEM]. Los Angeles: Sage; 2014.
[33] Schloderer M, Ringle C, Sarstedt M. Einführung in die varianzbasierte Strukturgleichungsmodellierung. Grundlagen, Mo-dellevaluation und Interaktionseffekte am Beispiel von SmartPLS. In: Schwaiger M, Meyer A, editors. Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende. München: Vahlen, pp.573–602, 2009
[34] Eberl M. Formative und reflektive Indikatoren im Forschungsprozess: Entscheidungsregeln und die Dominanz des reflektiven Modells.
[35] Gefen D, Straub D, Boudreau M-C. Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems, p.4, 2000
[36] Garson D. Partial Least Squares: Regression & Structural Equation Models. Asheboro, North Carolina: Statistical Associates Publishing; 2016
[37] Peikari,Hamidreza&Banazadeh,Babak. The Relationship between Information Security Awareness and the Intention to Violate Information Security with the Mediating Role of Individual Norms and Self-control.Journal of Strategic Rssearch on Social Problems. Vol. 7, Issue 4, No. 23, pp. 7-10,2019 (in Persian) Doi: 10.22108/ssoss.2019.108446.1174
[38]Hasanzadeh,Mohammad;Karimzadeganmoghaddam,Davood &Jahangiri,Narges.Providing a conceptual framework for evaluating probabilities and educating knowledge about information security of users.Journal of Information Systems and Services.Vol 1.No .2. pp.1-16, 2012(in Persian)
[39] Rodrigues Cardoso Waldson, Marco Silva João and Admilson Ribamar Lima Ribeiro. AN EXPERT SYSTEM AS AN AWARENESS TOOL TO PREVENT SOCIAL ENGINEERING ATTACKS IN PUBLIC ORGANIZATIONS International Journal on Cybernetics &Informatics,Vol.12,No.5.p.64,2023.https://doi.org/10.19044/esj.2023.v19n1p238
[40] Hoseiny.seyyedhasan;Majidi ghahroody.Nasim; Investigating The Effect of Social Engineering Techniques onEmployees Vulnerability (Case study: Tehran Municipality Employees). Scientific Journal of Electronical & Cyber Defence Vol. 11, No. 4,p.33,2023. https://dorl.net/dor/20.1001.1.23224347.1402.11.1.3.4 (in Persian)
[41] Asker. Hamida& Tamtam. Abdalmonem; An Investigation of the Information Security Awareness and Practices among Third Level Education Staff, Case Study in Nalut Libya. European Scientific Journal; Vol.16, No.15,p.30.2020 ,Doi:10.19044/esj.2020.v16n15p20.

Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 3, Autumn 2024, Serial No. 47
ISSN: 2322-4347 , E-ISSN: 2980-8979

The role of employee information security awareness in preventing social engineering Attacks
[Case example: Tehran Municipality employees]

S.H. Hosseini[1], N. Majidi[2*]

[2*]Assistant Professor, Islamic Azad University, Central Tehran Branch, Tehran, Iran

(Received:2024 /05/16, Revised: 2024/08/30, Accepted: 2024/09/27, Published: 2024/10/22)

DOR:https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.4.6

Abstract

Social engineering is a form of attack that seeks to trick employees into revealing their confidential information or performing actions on their behalf that threaten the security of the organization. The purpose of this article is to study the organizational and individual factors that influence employees' information security awareness and how this prevents social engineering attacks. This research was conducted on 1322 employees of Tehran Municipality. Awareness of information security was confirmed as one of the main factors in ensuring information security and raising the level of information security awareness as an important factor in protecting the organization against possible attacks. The theory of rational action and its expanded theory, i.e. the theory of planned behavior, were used in this study. 12 hypotheses were designed based on the opinions of experts and previous research, and the survey showed that six of the hypotheses were confirmed, three of them were partially confirmed, and three of them were rejected. The results of the research showed that information security policies, security awareness, training and skill enhancement programs and the effect of awareness on the insight and motivation of employees and the effect of perceptual behavior control on the motivation of employees in dealing with social engineering have significant effects in preventing the occurrence of social engineering. . The relationship between leadership, trust and risky behaviors with information security awareness was also measured and a weak relationship was found between them.

Keywords: : awareness of information security, social engineering, subjective norm, perceptual behavior control, information security policies

Publisher: Imam Hussein University Authors

**Corresponding Author Email: nas.majidi_gahrodi@iauctb.ac.ir*