Scientific Journal of Electronical & Cyber Defence
Vol. 11, No. 1, Spring 2023, Serial No. 41

Investigating The Effect of Social Engineering Techniques on Employees Vulnerability (Case study: Tehran Municipality Employees)

S. H. Hoseini,N. Majidi Ghahroodi*

* Assistant Professor, Central Tehran Branch, Islamic Azad University, Tehran, Iran

(Received: 03/04/2021, Accepted: 18/01/2022)

ABSTRACT

Social engineering is the art of deceiving people in a way that no use of force and threat, something to do or provide that information to social engineer . Social engineering can follow self-interest or organizational or national interest. Hackers, criminals, spies, saboteurs and ... all use social engineering to achieve their goals .social engineer uses Various techniques. In this study, the effect of this techniques on the vulnerability of people looked at the combined method (qualitative and quantitative) to measure this effect .First, various social engineering techniques as well as their vulnerability conducted by reviewing previous research and the interviewing with the experts in the field of engineering social was obtained and different techniques in a variety of technical, social, physical and technical – social were categorized. Afterwards in quantitative stage, By creating a questionnaire and various Items In the form of Likert scale and Provide the questionnaire to the target community(Employees of Tehran Municipality) The degree of vulnerability of people to a variety of social engineering techniques was obtained. It was found vulnerability of the target population is more than to the techniques of technical, social, technical – social and physical respectively . to prevent social engineering, human –driven and technology –based solutions were proposed that human –centered mainly on training personnel and IT solutions based on the provision of the right equipment, computers and creating a right information access cycle in organizations.

Keywords: Social engineering, Vulnerability, Communication security, Deception, Tehran municipality.

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

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۱، بهار ۱۴۰۲، ص ۳۱- ۴۶

علمی – پژوهشی

بررسی تأثیر روش‌های مهندسی اجتماعی بر آسیب‌پذیری کارکنان (نمونه موردی: کارمندان شهرداری تهران)

سیدحسن حسینی[۱]، نسیم مجیدی قهرودی[۲*]

۱-دانشجوی دکترای تخصصی علوم ارتباطات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران، ۲- استادیار، گروه ارتباطات، روزنامه‌نگاری و رسانه، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران

(دریافت: ۱۴۰۰/۱۰/۱۴، پذیرش: ۱۴۰۱/۰۳/۲۵)

چکیده

مهندسی اجتماعی هنر فریب انسان‌ها به‌گونه‌ای است که بدون استفاده از زور و تهدید، اقدامی را انجام دهند یا اطلاعاتی را ارائه دهند که موردنظر مهندس اجتماعی است. مهندس اجتماعی می‌تواند منافع شخصی، سازمانی یا ملّی را تهدید کند. نفوذگران، کلاهبرداران، جاسوسان، خرابکاران و ... همگی از مهندسی اجتماعی برای پیشبرد اهدافشان بهره می‌برند. مهندس اجتماعی از روش‌های مختلفی بهره می‌برد. در این تحقیق به تأثیر این روش‌ها بر آسیب‌پذیری کارکنان پرداختیم و از روش ترکیبی (کیفی و کمّی) برای سنجش این تأثیر استفاده شد. ابتدا روش‌های مختلف مهندسی اجتماعی با بهره‌برداری از مرور تحقیقات صورت‌گرفته قبلی و استفاده از نظرات کارشناسان حوزه مهندسی اجتماعی احصاء گردید و روش‌های مختلف در انواع فنی، اجتماعی، فیزیکی و فنی - اجتماعی دسته‌بندی شدند. سپس در مرحله کمّی با ایجاد گویه‌های مختلف در قالب طیف لیکرت و ارائه پرسش‌نامه به جامعه هدف (کارمندان شهرداری تهران)، میزان آسیب‌پذیری افراد نسبت به هرکدام از روش‌ها به‌دست‌آمده و در نهایت با میانگین‌گیری از پاسخ‌های ارائه شده میزان آسیب‌پذیری کل افراد نسبت به انواع روش‌های مهندسی اجتماعی حاصل شد. مشخص شد آسیب‌پذیری جامعه هدف به ترتیب نسبت به روش‌های فنی، اجتماعی، فنی - اجتماعی و فیزیکی بیشتر است. جهت پیشگیری از وقوع مهندسی اجتماعی نیز راهکارهای انسان‌محور و فناوری محور پیشنهاد شد.

کلیدواژه‌ها: مهندسی اجتماعی، آسیب‌پذیری، امنیت ارتباطات، فریب.

۱- مقدمه

در چند دهه گذشته ابزارهای ارتباطی رشد قابل‌ملاحظه‌ای یافته‌اند و این امر سرعت و سهولت ارتباط را ساده‌تر نموده است. این پدیده امکانات مفید زیادی را در اختیار افراد قرار می‌دهد. اما علاوه بر مزیت‌های فراوان این امر، بر خطرات و تهدیدات نیز به همان اندازه افزوده شده است. آسیب‌پذیری‌های ارتباطی افراد چه در فضای حقیقی و چه در فضای مجازی در حال افزایش است که یکی از علت‌های آن عدم آشنایی افراد با این خطرات است. مهندسی اجتماعی یکی از تهدیداتی است که در دو دهه گذشته خود را بیش‌ازپیش نمایان کرده است. گسترش شبکه‌های مجازی و حداکثرسازی میزان ارتباطات و نمایان ساختن وجوه مختلف انسان در آن، موجب شده مهندسان اجتماعی با ایجاد شناخت مناسب از قربانیان خود، بهترین سناریو را برای سوءاستفاده از آنها طراحی کنند. این مهندسان اجتماعی می‌توانند دولت‌ها، سرویس‌های اطلاعاتی، شرکت‌های رقیب و یا افراد سودجو باشند. حملات مهندسی اجتماعی یکی از خطرناک‌ترین حملات در سرتاسر جهان است [۱]. ماهیت انسان ایجاب می‌کند که به دیگران کمک کرده و به دوستان و اطرافیانش اعتماد کند. مهندس اجتماعی با استفاده از همین امر، رابطه‌ای مبتنی بر اعتماد را با شخص هدف ایجاد کرده و سپس از این اعتماد در جهت رسیدن به اهداف از پیش تعیین شده سوءاستفاده می‌کند (همان). مهندسی اجتماعی به دانش فنی زیادی نیاز ندارد اما نیازمند فهم و درک درست از ذهن انسان‌هاست[۲]. مهندسی اجتماعی پیچیده‌تر از اجرای مجموعه‌ای از حملات سایبری است و نیازمند ابزارهای متنوعی است؛ این اهرم‌ها شامل روش‌ها و فناوری‌های جدید و پیشرفته، تحلیل اطلاعات منابع آشکار، تحلیل شبکه‌های اجتماعی، تحلیل روان‌شناختی، تحلیل احساسات و تمایلات افراد می‌شود [۳].

بخش زیادی از سوءاستفاده‌ها و افشای اطلاعات در فضای حقیقی یا مجازی به علت عدم آشنایی و شناخت افراد نسبت به آسیب‌ها و اثرات اقداماتشان صورت می‌گیرد که این افشای اطلاعات می‌تواند اثرات سویی در سطوح فردی، سازمانی و ملی داشته باشد. ایمیل و پیام‌رسان‌های فوری، خدمات اینترنتی و دیگر سایت‌های شبکه‌های اجتماعی بخشی از زندگی روزانه در ارتباطات کاری و شخصی شده‌اند [۴]. یک تمایل روزافزون به سمت استفاده کارکنان از ابزارهای ارتباطی برای موارد کاری هم در محیط کار و هم در منزل وجود دارد. در اکثر اوقات، کاربران

* رایانامه نویسنده مسئول: Nassim_majidi2000@yahoo.com

ناشر: دانشگاه جامع امام حسین (ع)

به افرادی که با آنها ارتباط برقرار می‌کنند اعتماد می‌کنند؛ حتی در زمانی که تنها شناخت آنها در قالب یک ایمیل یا پروفایل مجازی است. در سال‌های اخیر، آسیب‌پذیری‌های امنیتی در ارتباطات آنلاین و کانال‌های به‌اشتراک‌گذاری داده‌ها اغلب موجب سوءاستفاده و افشای اطلاعات حساس شده است.

عواطف، احساسات و نقاط ضعف انسان است که به‌عنوان ابزار نفوذ مهندسان اجتماعی مورداستفاده قرار می‌گیرد. یکی از دلایل موفقیت مهندسی اجتماعی آن است که ارزیابی و بررسی کلیه ارتباطات برای کاربران مشکل است. علاوه بر این، اعتبارسنجی نیازمند سطحی از تخصص فنی است که اکثر کاربران فاقد آن هستند. آنچه این مشکل را بیشتر می‌کند آن است که تعداد کاربرانی که دارای دسترسی به اطلاعات خاص هستند زیاد بوده و همین امر زمینه لازم برای حملات مهندسان اجتماعی را فراهم می‌کند[۵].

کوچک‌ترین نشت اطلاعات حیاتی یک سازمان شاید به بزرگ‌ترین تهدید برنامه‌های سازمان تبدیل شود. حتی خانواده، دوستان و همکاران می‌توانند جزو اهداف مهاجمان باشند زیرا آنها اغلب اوقات سعی می‌کنند از طریق اشخاص ثالث اطلاعات حیاتی را به دست آورند[۶].

در این مقاله، ما ضمن مطرح‌کردن روش‌های مختلف مهندسان اجتماعی میزان آسیب‌پذیری کارکنان به‌ویژه کارکنان شهرداری تهران نسبت به حملات مهندسی اجتماعی را ارزیابی خواهیم کرد. چگونگی آسیب‌پذیری روانی، ارتباطی و رفتاری کارکنان نسبت به روش‌های به کار گرفته شده از جانب مهندسان اجتماعی چه در فضای مجازی و چه در فضای حقیقی اصلی‌ترین مسئله موردتوجه در این مقاله است.

۱-۱- اهمیت و ضرورت تحقیق

بسیاری از سازمان‌ها و شرکت‌ها در آموزش کارکنانشان نسبت به حملاتی که می‌تواند به علت عدم دانش آنها صورت گیرد ناموفق بوده‌اند. بخشی از علت این عدم موفقیت می‌تواند ناشی از عدم آگاهی مدیران و رؤسای دولت‌ها، سازمان‌ها، شرکت‌ها و نهادها نسبت به پدیده مهندسی اجتماعی و تبعات زیان باری است که می‌تواند برای آنها در سطوح فردی، سازمانی، ملی و حتی بین‌المللی به همراه داشته باشد. بنابراین، آگاهی از ابزارهای مورداستفاده مهاجمان توسط افراد مختلف به‌ویژه کارکنان سازمان‌ها و بالاخص کارکنان مراکز حساس می‌تواند از خروج داده جلوگیری کرده و هزینه‌ها را کاهش می‌دهد.

سنجش میزان آسیب‌پذیری کارکنان و نیز کمیت و کیفیت آن می‌تواند نقاط ضعف و آسیب‌زای سازمانی و انسانی سازمان‌ها را مشخص کرده و این امر می‌تواند به گسترش راهکارها و سیاست‌های لازم برای حفظ منابع، داده‌ها و دستاوردهای سازمان‌ها منتج شود. علاوه بر این، این تحقیق می‌تواند به لحاظ روش‌شناسی مسیری را برای سنجش آسیب‌های مختلف سازمانی برای دیگر محققان فراهم کند.

تشریح و تعریف موضوع مهندسی اجتماعی و ابعاد مختلف آن؛

تشریح روش‌های مختلف مهندسان اجتماعی

شناخت آسیب‌های اجتماعی و روانی که می‌تواند بستری برای حملات مهندسی اجتماعی باشد؛

جلوگیری و پیشگیری از آسیب‌های امنیتی مردم و سازمان‌ها؛

احصای آسیب‌پذیری‌های ارتباطی مردم به‌ویژه کارمندان؛

ایمن‌سازی ارتباطات افراد در فضای مجازی و حقیقی از طریق شناخت آسیب‌پذیری‌ها.

۱-۲- اهداف ویژه و کاربردی

شناخت میزان نقش و تأثیر مهندسی اجتماعی بر سازمان‌ها به‌ویژه شهرداری تهران؛

افزایش آگاهی مردم و به‌ویژه کارمندان در خصوص تهدیدات مهندسی اجتماعی.

۱-۳- فرضیه‌ها

به نظر می‌رسد باتوجه‌به جدید بودن موضوع و عدم آشنایی اکثریت کارکنان نسبت به موضوع مهندسی اجتماعی، روش‌ها و روش‌های مختلف آن، میزان بالایی از کارکنان نسبت به روش‌های مهندسی اجتماعی ناآگاه و در نتیجه آسیب‌پذیر باشند. بنابراین، به نظر می‌رسد روش‌های مهندسی اجتماعی تأثیر معناداری بر آسیب‌پذیری رفتاری و روانی کارکنان و به‌تبع آن آسیب‌پذیری سازمان داشته باشند. به نظر می‌رسد مهم‌ترین مسئله در آسیب‌های ارتباطی کارکنان، عدم آموزش و شناخت آنها نسبت به روش‌های تهدیدات به‌ویژه در خصوص موضوع مهندسی اجتماعی است و همین مسئله میزان آسیب‌پذیری آنها را در برابر خطرات مهندسی اجتماعی بالا برده است.

۱-۴- تعریف مهندسی اجتماعی

مهندسی اجتماعی به‌عنوان سومین حرفه قدیمی دنیا شناخته شده که تنها فاحشگی و جاسوسی مشاغل قدیمی‌تر از آن محسوب می‌شوند. درک مهندسی اجتماعی معمولاً با دروغ‌گویی به مردم برای گرفتن اطلاعات، یا بازیگر خوب‌بودن یا فریب مردم مرتبط است[۷].

مهندسی اجتماعی هنر فریب کاربران برای سوءاستفاده از اطلاعات یا سیستم‌های اطلاعاتی آنهاست. مهندس اجتماعی به‌جای استفاده از حملات فنی به سیستم‌ها، انسان‌های دارای دسترسی به اطلاعات را هدف قرار داده و آنها را فریب داده تا اطلاعات محرمانه یا شخصی خود را ارائه دهند یا حملات خود را از طریق تأثیر و اقناع انجام دهند[۸].

مهندسی اجتماعی مجموعه روش‌ها و ویروس‌ها به‌اضافه فریب مردم و سوءاستفاده از عدم آگاهی آنها از سیاست‌ها و رویه‌های امنیت اطلاعات است[۹].

کریستوفر هدنگی، متخصص حرفه‌ای بحث مهندسی اجتماعی است. او مهندسی اجتماعی را به‌عنوان " عمل دست‌کاری یا فریب یک فرد برای متقاعدکردن او به انجام عملی که ممکن است به نفع او نباشد" تعریف می‌کند[۷].

کوین میتنیک را اغلب به‌عنوان پدر مهندسی اجتماعی مدرن می‌دانند. او مهندسی اجتماعی را این‌گونه تعریف می‌کند:" مهندسی اجتماعی از تأثیر و اقناع برای فریب مردم استفاده می‌کند. مهندسی اجتماعی قادر است اطلاعاتی را با استفاده یا بدون استفاده از فناوری از افراد به دست آورد"[۱۰].

تلاش موفق یا ناموفق برای اثرگذاری بر فرد به‌منظور آشکارکردن اطلاعات یا انجام رفتاری که منجر به دسترسی غیرمجاز با افشای غیرمجاز اطلاعات یک سیستم، شبکه یا داده‌ها شود تعریف دیگری از مهندسی اجتماعی است[۱۱]. یا در تعریف دیگر مهندسی اجتماعی به‌عنوان هنر بهره‌برداری از ویژگی‌های انسانی برای دستیابی به اطلاعات عنوان شده است[۱۲].

آسیب‌پذیری‌های رفتاری در برابر مهندسی اجتماعی

همان‌طور که قبلاً نیز عنوان شد تا زمانی که فرد یا سازمان هدف از خود ضعف یا آسیبی نشان ندهد مهندس اجتماعی قادر به پیشبرد اهداف خود نیست. بسیاری از این آسیب‌ها ریشه در رفتارهای فردی یا اجتماعی افراد یا فرهنگ حاکم بر جامعه یا سازمان داشته که می‌تواند منشأ سوءاستفاده از افراد در مواردی همچون کلاهبرداری، سرقت، مهندسی اجتماعی و ... باشد. برخی از این آسیب‌پذیری‌ها شامل زودباوری و اعتماد بی‌جا، تنبلی، پرحرفی، عدم داشتن مهارت نه گفتن، عدم داشتن تفکر انتقادی، عجول بودن، عدم رازداری، رودربایستی، طمع، کنجکاوی بیجا، ترس، غفلت، قانون‌گریزی و خود افشایی می‌شود.

۲- روش‌های مهندسی اجتماعی:

منظور از روش‌ها و فنونی است که برای به دام انداختن قربانیان مورداستفاده قرار می‌گیرند. روش‌های مهندسی اجتماعی به چهار دسته فنی محور، اجتماعی محور، فیزیکی محور و فنی - اجتماعی محور تقسیم می‌شوند.

۲-۱- روش‌های فنی محور: حملاتی هستند که مبتنی بر ابزار و دانش فنی مهندس اجتماعی است. مثلاً مهاجمان اغلب از موتورهای جستجو برای جمع‌آوری اطلاعات شخصی درمورد قربانیان آتی استفاده می‌کنند. یا ابزارهایی نیز وجود دارند که می‌توانند اطلاعات را از منابع اینترنتی مختلف جمع‌آوری کنند که شامل موارد ذیل است:

۲-۱-۱- اسنیفینگ[۲]: اسنیفینگ به معنای رصد همه داده‌هایی است که از طریق سیم‌ها منتقل شده یا گاهی اوقات از طریق هوا و شبکه‌های بی‌سیم منتقل می‌شوند. نفوذگران در حال حاضر از اسنیفینگ برای اسکن آی‌دی‌ها و رمز عبورهای روی سیم‌ها استفاده می‌کنند. رمزگذاری یکی از راه‌های جلوگیری از حملات اسنیفینگ است[۱۳].

۲-۱-۲- حملات بدافزار[۳]: بدافزار رایج‌ترین تهدید خارجی اکثر سازمان‌ها و گروه‌ها محسوب شده که خسارات زیادی را به همراه دارد. بدافزار اغلب برای سوءاستفاده از اطلاعات و داده‌هایی که به‌راحتی قابل‌بهره‌برداری بوده مثل اطلاعات مربوط به ورود سیستم، شماره‌های حساب بانکی و کارت اعتباری و در برخی موارد اسرار تجاری استفاده می‌شود. در مرحله اول نفوذ بدافزار، کاربر ممکن است یک ایمیل را دریافت کند تا مجرم سایبری بتواند به اطلاعات کاربر دسترسی یابد یا بتواند به سیستم تحت کنترل کاربر وارد شود. هنگامی که مجرم سایبری ارتباط را با کاربر یا سیستم آغاز کرد، می‌تواند از دیگر ابزارهایی که می‌توانند دسترسی عمیق‌تری را به منابع سیستم فراهم کرده، بهره‌برداری کند[۱۴].

۲-۱-۳- حملات باج‌افزار[۴]: حملات باج‌افزار، دسترسی به داده‌ها و فایل‌های قربانی را از طریق رمزگذاری آنها محدود می‌کند[۱۵] و قربانی تهدید می‌شود که این فایل‌ها به‌صورت عمومی منتشر می‌شود مگر آنکه باج بپردازد. پیامدهای یک حمله باج‌افزار می‌تواند هزینه بیشتری از خود باج دادن داشته باشد[۱۶]. خسارات شرکت‌ها و سازمان‌هایی که تحت‌تأثیر حملات باج‌افزار قرار گرفته، به علت خسارات به وجود آمده برای شرکت، مشتریان، داده‌ها و بهره‌وری آن تا سالیان سال باقی می‌ماند. حمله باج‌افزار معمولاً شامل شش مرحله است: ۱. ایجاد بدافزار ۲. راه‌اندازی و به‌کارگیری ۳. نصب ۴. فرماندهی و کنترل ۵. تخریب ۶. اخاذی[۱۷]. هنگامی که یک حمله بدافزار روی رایانه اجرا می‌شود، قربانی تنها سه انتخاب دارد: ۱. پرداخت باج برای بازگرداندن فایل‌های رمزگذاری شده ۲. تلاش برای بازگرداندن فایل‌ها از طریق نسخه‌های پشتیبان ۳. ازدست‌دادن فایل‌ها و داده‌ها بعد از امتناع از پرداخت باج[۱۸].

۲-۱-۴- حملات فارمینگ[۵]: فارمینگ نوعی حمله سایبری مهندسی اجتماعی است که در آن مجرمان کاربران اینترنت که به دنبال دستیابی به یک وب‌سایت خاص هستند را به سمت

[2] Sniffing
[3] Malware
[4] Ransomware
[5] Pharming

وب‌سایت های جعلی هدایت می‌کنند. هدف طراحی این سایت‌های جعلی سرقت اطلاعات هویتی و شخصی قربانی و اطلاعات ورود به سیستم است یا به دنبال نصب بدافزارهای فارمینگ روی رایانه‌هایشان هستند. مهاجم ترافیک یک وب‌سایت خاص را با مسیردهی مجدد آن به یک وب‌سایت جعلی دیگر سرقت کرده تا اطلاعات را به دست آورد [۱۹]. آنچه که حملات فارمینگ را در میان حملات آنلاین خطرناک‌تر می‌سازد آن است که این روش نیازمند حداقل اقدام از جانب قربانی است[۲۰].

۲-۱-۵- **حفاری آب**[6]: نام حفاری آب از صیادان و شکارچیانی الهام گرفته که نزدیک گودال‌های آب کمین کرده و منتظر فرصتی برای حمله به صید بالقوه هستند. در حمله حفاری آب، شکارچی در وب‌سایت‌های خاصی که برای شکارهایشان جذاب هستند کمین کرده و منتظر فرصتی برای آلوده ساختن آنها با بدافزارهایی که این اهداف را آسیب‌پذیر ساخته می‌مانند. به‌عبارت‌دیگر نفوذگران سایت‌های آسیب‌پذیر را آلوده ساخته تا یک موضوع یا طعمه‌ای که برای اهدافشان جذاب است را در آنجا به اشتراک بگذارد و سپس قربانیان را به سمت اپلیکیشن یا سایتی که حاوی بدافزار است بکشانند. هدف حمله آن است که رمز عبور و نام کاربری که کاربر استفاده می‌کند و ممکن است آنها را در وب‌سایت‌های دیگر هم استفاده کند به دست آید یا اینکه رایانه قربانی را آلوده سازند و به شبکه سازمان یا شرکتی که قربانی به آن متصل است دسترسی یابند[۲۱].

۲-۲- روش‌های فیزیکی محور: روش‌های فیزیکی، روش‌هایی هستند که مهاجم برخی از اقدامات فیزیکی را برای جمع‌آوری اطلاعات در مورد قربانی آتی انجام می‌دهد[۲۲].

۲-۲-۱- زباله‌گردی[7]: این روش به سرقت اسناد، مدارک و هویت مرتبط است که شامل جمع‌آوری اسناد حساس از جمله اطلاعات کارت اعتباری، دسترسی به اسناد محرمانه، فهرست افراد و چارت‌های سازمانی از سطل‌های زباله یا تجهیزات ازکارافتاده مثل ابزارها و وسایل رایانه‌ای کهنه، ابزارهای ذخیره‌ساز، سی‌دی‌ها و دی‌وی‌دی‌ها می‌شود[۲۳].

۲-۲-۲- سرک‌کشی[8]: سرک‌کشی در جایی است که سارقان اطلاعات و داده‌های شخصی را با نگاه‌کردن به صفحه لپ تاب، تلفن همراه، تبلت، عابربانک و ... از روی شانه افراد انجام می‌دهند. آنها می‌توانند شماره پین کد تلفن همراه، رمز عبور و ... افراد را این‌گونه به دست آورند. آنها ممکن است حتی در یک فاصله مطمئن از قربانی بایستند و با تفسیر حرکات انگشت که در حال تایپ شماره‌ها روی کیبورد است اطلاعات را به دست آورند. مهندسان اجتماعی حتی ممکن است از دوربین‌های کوچک یا دوربین‌های موجود روی تبلت یا تلفن همراهشان برای دیدن صفحه تلفن همراه یا تبلت فرد استفاده کنند. آنها حتی ممکن است در زمانی که فرد در پشت تلفن در حال خواندن شماره‌های کارت پشت تلفن بوده صدای فرد را شنود کنند[۲۴].

۲-۲-۳- حملات دنباله‌روی یا کولی گرفتن[9]: حملات دنباله‌روی که کولی گرفتن یا دسترسی فیزیکی نیز نامیده شده، شامل دسترسی پیداکردن به یک ناحیه یا ساختمان از طریق تعقیب افرادی است که دارای مجوزهای امنیتی برای ورود به آن مکان هستند. آنها به مهاجمان اجازه می‌دهند تا به ساختمان‌ها به‌صورت غیرمجاز دسترسی یابند. برای مثال، مهاجمان از قربانی می‌خواهند تا در را برای آنها باز نگه دارد زیرا آنها کارت شناسایی شرکت یا کارت هوشمندشان را فراموش کرده‌اند[۲۵]. مهاجم ممکن است پشت در یک ساختمان یا شرکت بایستد و بعد از خروج یکی از کارکنان یا ساکنین به بهانه آشنا بودن با یکی از ساکنین یا مهمان بودن یا کارمند شرکت بودن وارد آنجا شود. یا اینکه جعبه بزرگی را در دستش داشته باشد و همزمان با کسی که وارد یک ساختمان می‌شود وارد شود و از او بخواهد در را برایش باز نگه دارد[۱۶].

۲-۲-۴- حملات سرقت انحرافی[10]: در قدیم سارقان از این روش برای متقاعدکردن یک راننده بار برای تغییر مسیر یا سفر به مکان اشتباهی یا دادن بسته یا بار به شخص دیگر(غیر از شخص اصلی تحویل گیرنده) استفاده می‌کردند. در سرقت انحرافی انلاین، سارق داده‌های حساس را از طریق فریب قربانی برای ارسال اطلاعات یا به‌اشتراک‌گذاری آن با افراد دیگر(سارقان) سرقت می‌کنند. سارقان یا مهندسان اجتماعی ممکن است لباس مأمور، راننده یا گیرنده بسته یا بار را پوشیده و محصول را از مبدأ دریافت کنند[۲۶].

۲-۳- روش‌های اجتماعی محور: از طریق ارتباط با قربانیان و بازی با احساسات و روان آنها انجام می‌شود[۲۷]. در این نوع حملات، مهاجمان به روش‌های روانی اجتماعی متکی هستند. برای افزایش شانس موفقیت چنین حملاتی، مرتکبان اغلب تلاش می‌کنند تا رابطه خود با قربانیان آتی‌شان را افزایش و تعمیق دهند[۲۸].

۲-۳-۱- تظاهر به خودی بودن[11]: مهندس اجتماعی می‌تواند در پوشش یک پیمانکار، تعمیرکار یا کارگر یا هر کسی که بتواند اعتماد کارکنان را جلب کرده وارد سازمان شده و اطلاعاتی مثل رمز عبور یا اطلاعات سازمان را به دست آورد[۲۹].

[6] Water holing
[7] dumpster diving
[8] shoulder surfing
[9] Piggybacking
[10] Diversion theft
[11] Insider impersonation

۲-۳-۲- همدلی و همدردی[12]: ایزنبرگ و دیگران همدردی را احساس غم و دلهره نسبت به فرد نیازمند و دچار مشکل تعریف کرده، که بر پایه مقایسه موقعیت و شرایط فردی با فرد دیگر تجربه می‌شود. در حالی که، همدلی شامل چنین تجربه هیجانی نیست و بیشتر سعی در قراردادن خود به‌جای فرد دیگر و تصور تجربه اوست[۳۰]. در حوزه مهندسی اجتماعی، مهاجم خود را با قربانی همدل نشان داده و با او ممکن است همدردی کند مانند کسی که نزدیکانش را از دست داده یا بیمار است و از این طریق سعی می‌کند اعتماد او را جلب کند.

۲-۳-۳- ایجاد ترس و تسلط[13] : مهاجم سعی می‌کند با ایجاد استیلا بر هدف یا ترساندن او فرد هدف را جهت انجام اقدام مورد نظرش ترغیب کند. به‌عنوان مثال مهندس اجتماعی با فرد هدف تماس تلفنی برقرار کرده و خود را جای یک مقام مسئول بالاتر جا می زند.کارکنان در برابر کسانی که قدرت داشته باشند به راحتی تسلیم می‌شوند و در صورتی که درخواستی از آنها نماید که ممکن است غیرقانونی باشد ممکن است از ترس توبیخ یا تنبیه شدن یا ازدست‌دادن شغل، آن کار را انجام دهند. مهندسان اجتماعی از اصل تسلط استفاده کرده تا اهدافشان را برای انجام اقدامات موردنظر آنها ترغیب کنند[۲۹] یا اینکه مهندس اجتماعی به‌ویژه در فضای مجازی تبلیغ کالا یا خدماتی را بکند که برای استفاده یا خرید از آن تنها چند ساعت باقی مانده است. قربانی ممکن است با ترس ازدست‌دادن آن کالا یا خدمت یا ... فریب مهندس اجتماعی را خورده و اقدام به وارد کردن اطلاعات شخصی ، مالی و .. یا کلیک روی لینک موردنظر کند.

۲-۳-۴- زیرپاکشی[14]: اخذ اطلاعات از طریق گفتگو با فرد به شکلی که وی متوجه نیت واقعی گفتگو کننده نشده و ناخودآگاه اقدام به افشای اطلاعات نماید. زیرپاکشی به معنای بیرون کشیدن حرف از کسی است یا کسی را به طور منطقی وارد شرایطی کردن که حقایقی را بیان کند. این روش با هدفی معین در مورد اشخاصی صورت می‌گیرد که معمولاً دسترسی به اطلاعات مورد نیاز مهندس اجتماعی را دارند. ستایش و تمجید کردن، چاپلوسی، عصبانی‌کردن فرد، طرح سؤالات مکرر، مظلوم‌نمایی، یک دستی زدن و ... از جمله روش‌های به کار گرفته شده مهندسان اجتماعی برای انجام زیرپاکشی است[۷].

۲-۳-۵- شبیه‌سازی[15]: ما تمایل داریم به افرادی که به ما از جهات مختلف اعتقادی، اخلاقی، اجتماعی و ... شباهت دارند بیشتر اعتماد کنیم و ارتباط برقرار کنیم. اما میان شباهت واقعی با شباهت ظاهری یا شباهتی که در ذهن فرد است تفاوت وجود دارد. شباهت ادراک شده تأثیر بیشتری بر روابط فرد نسبت به طرف مقابل نسبت به شباهت واقعی دارد[۳۱]. در مهندسی اجتماعی روش تشبیه قربانی به خود توسط مهندس اجتماعی را شبیه‌سازی می نامند. ایجاد شباهت واقعی یا کاذب با قربانی از نوع ظاهر، وضعیت خانوادگی، تحصیلی، اعتقادات ملی و مذهبی، سلیقه و ... از جمله روش‌های مورداستفاده مهندسان اجتماعی است[۷].

۲-۳-۶- ایجاد یک حس اضطرار دروغین با ادعای عرضه محدود یا همان ایجاد حس کم‌یابی[16]: مهندسان اجتماعی ممکن است از کم‌یابی برای ایجاد حس فوریت یا اضطرار در تصمیم‌سازی استفاده کنند. این فوریت اغلب می‌تواند منجر به دستکاری یا تأثیرگذاری بر فرایند تصمیم‌سازی شود که به مهندس اجتماعی این امکان را می‌دهد که اطلاعات ارائه شده به قربانی را کنترل کند. اگر شخصی دریابد که چیزی نادر یا کم‌یاب بوده یا مقدار آن کم بوده یا دیگر تولید نمی‌شود ارزشش افزایش می‌یابد[۳۲]. معمولا آگهی‌های بازرگانی مثل فروش سه‌روزه، برای زمان محدود، حراج به علت تغییر شغل و آخرین روز نظر مردم را جلب می‌کند چون به گمانشان دیگر چنین فرصتی برای آنها به وجود نمی‌آید. کمیابی نوعی حس اضطرار برای تصمیم‌گیری در دل هدف را ایجاد می‌کند. این حس باعث می‌شود که مهندس اجتماعی بر فرایند تصمیم‌گیری هدف تأثیر گذاشته و کنترل اطلاعات را در دست بگیرند[۳۳]

۲-۳-۷- عمل متقابل یا مدیون‌سازی(جبران کردن)[17]: دادن یک امتیاز یا تسهیلات یا امکان ویژه از طرف مهاجم به هدف و در ازای آن هدف به جبران کردن آن اقدام می‌کند[۳۴]. معمولاً بازگرداندن لطف و قانون عمل متقابل به‌صورت ناخودآگاه صورت می‌گیرد. مهندس اجتماعی سعی می‌کند اقدامی مادی یا معنوی را برای قربانی خود انجام دهد و سپس درخواستی را از قربانی مطرح می‌کند تا او هم اقدامی که مهندس اجتماعی انجام داده را جبران کند[۲۳].

۲-۳-۸- سند یا اجماع اجتماعی[18]: سند یا اجماع اجتماعی به حالت فیزیولوژیکی اطلاق می‌شود که در آن افراد نمی‌توانند شکل درستی از رفتار را در یک موقعیت اجتماعی نشان دهند. مهندسان اجتماعی از سند اجتماعی برای تحریف اهدافشان استفاده کرده و با بیان اینکه سایرین نیز همین رویه را درپیش گرفته آنها را به سمت دلخواهشان پیش می‌برند. مهندسان اجتماعی به اهدافشان می گویند که فلان فرد شناخته شده نیز در این موقعیت همین رفتار را نشان داده یا اینکه دیگران نیز این

[12] Sympathy
[13] Scare
[14] Elicitation
[15] Similarization
[16] Scarcity
[17] Reciprocating or Quid Pro Quo
[18] Social consensus

کالا را خریداری کرده فرد هدفشان را قانع می‌کنند تا اقدام مورد نظرشان را انجام دهند[۲۹].

۲-۴- روش‌های فنی-اجتماعی‌محور: روش‌های فنی-اجتماعی قدرتمندترین ابزار مهندسان اجتماعی محسوب می‌شوند که در آن مهاجم از حملات فنی و اجتماعی توأمان استفاده می‌کند[۳۵].

۲-۴-۱- اسپوفینگ[19]: اسپوفینگ به معنای فریب دیگران است؛ فریب کاربران رایانه‌هایی که اطلاعات را از منبعی دریافت کرده که توسط یک کاربر قانونی ارائه شده است. اسپوفینگ ایمیل به ایجاد پیام های ایمیل با آدرس فرستنده جعلی اشاره دارد. اسپوفینگ برای گمراه ساختن گیرنده‌ها در مورد منشا پیام‌ها انجام می‌شود تا آنها را متقاعد کند تا اقدامی را انجام دهند.اسپوفینگ می‌تواند به چند روش رخ دهد مثل اسپوفینگ آی پی، اسپوفینگ دی ان اس و اسپوفینگ آی آر پی[۳۶].

۲-۴-۲- مهندسی اجتماعی معکوس[20]: در این نوع حمله ، مهاجم اقدام به خرابکاری یا ایجاد اختلال در سیستم های رایانه ای هدف یا ایجاد مشکل در زندگی شخصی یا حرفه ای او کرده و بعد خودش را به‌عنوان منجی یا فردی که قادر به حل کردن آن مسئله یا مشکل است جا می زند مانند زمانی که مهندس اجتماعی اقدام به پنچر کردن ماشین یا اخلال در سیستم های رایانه ای فرد کرده و بعد با ارتباط گیری با او سعی می‌کند به‌عنوان یک دوست یا فردی که نیت خیرخواهانه‌ای داشته مشکلش را حل کند. این حمله شامل این مراحل است: به وجود آوردن یک مشکل مثل اختلال در شبکه؛ تبلیغ این که مهاجم تنها کسی است که می‌تواند این مشکل را حل کند؛ حل کردن مشکل در عین دستیابی به اطلاعات مورد نیاز و ترک مکان بدون این که از خود ردّپایی برجا بگذارد[۳۷].

۲-۴-۳- فیشینگ[21]: فیشینگ شامل تلاش یک مهاجم برای اغوای قربانیان برای وارد کردن اطلاعات حساسی همچون رمزهای عبور یا شماره‌های کارت اعتباری در یک وب‌سایت جعلی است که توسط مهاجم کنترل می‌شود[۳۸].حملات فیشینگ را می‌توان به پنج دسته تقسیم کرد: اسپیرفیشینگ، والینگ ، ویشینگ ، روبوکال‌ها و فیشینگ از طریق سوءاستفاده از ایمیل‌های تجاری.

اسپیرفیشینگ به فیشینگ خاصی که افراد یا گروه‌های منتخب خاص را هدف قرار داده اشاره دارد که از نام آنها برای ایجاد ارتباط استفاده می‌کند[۳۹].

والینگ یا صید نهنگ، نوعی حمله فیشینگ است که اشخاص و هویت‌های عالی‌رتبه در شرکت‌هایی که به آنها ماهی‌های بزرگ یا صیدهای بزرگ گفته می‌شود را هدف قرار می‌دهد[۴۰].

حملات ویشینگ به فیشینگ تلفنی اشاره دارد که افراد را فریب می‌دهد تا اطلاعات حساسشان را ارائه دهند؛ مثل تماس‌های جعلی که به‌ظاهر از جانب یک بانک معتبر گرفته شده است[۴۱].

فیشینگ از طریق روبوکال‌ها: حملات روبوکال‌ها، تماس‌های گسترده‌ای است که از جانب رایانه‌ها با اشخاص مورد هدفی که شماره‌تلفن آنها شناسایی شده برقرار می‌شود[۴۲]. این تماس‌ها با استفاده از سیستم تلفن گویا انجام شده تا هدف را مجاب کند که تماس از جانب یک بانک یا شرکت معتبر انجام شده است[۴۳].

فیشینگ سوءاستفاده از اخبار جعلی یا ایمیل و فایل آلوده: مهاجم بعد از به‌دست‌آوردن اطلاعات موردنیاز، یک ایمیل کاری که ظاهری کاملاً قانع‌کننده و قانونی دارد را برای یک کارمند معمولی ارسال می‌کند تا کارمند روی یک لینک کلیک کند یا ضمیمه ایمیلی را دانلود کند تا بتواند به شبکه شرکت یا سازمان دست یابد. جعل اخبار به‌ویژه در شبکه‌های اجتماعی برای کشاندن قربانیان به صفحات آلوده یا اخذ اطلاعات آنها یکی دیگر از روش‌های فیشینگ است. حملات پی‌دی‌اف هم یکی دیگر از ابزارهای فیشینگ محسوب می‌شود. حمله در قالب یک فایل پی‌دی‌اف ساده صورت می‌گیرد که حاوی یک هایپرلینک است که هنگامی که روی آن کلیک می‌شود، کاربر را به سمت وب‌سایت هدایت کرده یا سیستمش را آلوده به تروجان می‌کند. ایمیل‌های موسوم به ایمیل‌های نیجریه‌ای وجود دارد که برای فیشینگ از آنها استفاده می‌شود مثل این که شما برنده لاتاری شده‌اید ولی برای دریافت جایزه باید مبلغی را پرداخت کنید. وقتی آن مبلغ که ظاهراً ممکن است اندک باشد پرداخت می‌شود دیگر خبری از فرد ارسال‌کننده ایمیل نمی‌شود. هرزنامه‌ها یکی دیگر از ابزارهای فیشینگ است. ایمیل‌هایی که حاوی لینکی بوده که به یک فروشگاه اینترنت، سایت کلاهبرداری یا نرم‌افزارهای هرز متصل می‌شوند. آنها به طور خودکار کار کرده و قربانیان زیادی را هدف قرار می‌دهند[۱۴].

حملات اسمیشینگ: شامل ارسال پیام‌ها و متن‌های جعلی از طریق تلفن همراه برای قربانی و تأثیرگذاری بر وی است. کارایی حملات اسمیشینگ به این حقیقت وابسته است که قربانیان تلفن‌های همراهشان را هر جا و هرزمان با خودشان حمل می‌کنند. پیام متنی دریافتی می‌تواند حاوی بدافزار باشد[۴۱].

۲-۴-۴- جعل هویت[22]: جعل هویت هم در فضای حقیقی و هم در فضای مجازی انجام می‌شود. در فضای حقیقی کلاهبردار یا مهندس اجتماعی خود را جای شخصی جا می‌زند تا قربانی را وادار به انجام کار یا دادن اطلاعات نماید. در فضای مجازی نیز این جعل هویت وجود دارد. مطالعه انجام شده توسط سوفوس

[19] spoofing
[20] Reverse social engineering
[21] phishing
[22] Impersonation

که در سال ۲۰۰۷ منتشر شد و کاربران فیس‌بوک به‌صورت تصادفی انتخاب شده بودند نشان داد که تقریباً ۴۱ درصد کاربران شبکه‌های اجتماعی درخواست‌های دوستی از جانب پروفایل جعلی را پذیرفته‌اند[۴۴].

۲-۴-۵- حملات دستاویزسازی[۲۳]: حملات دستاویزسازی شامل طراحی سناریوهای جعلی و متقاعدکننده در جهت سرقت اطلاعات شخصی قربانی است. مهندسان اجتماعی بهانه یا دستاویزی پیدا کرده تا اعتماد قربانی نسبت به مهاجم را جلب نمایند. این دستاویز می‌تواند یک پیشنهاد برای ارائه یک خدمت یا گرفتن شغل باشد که درخواست‌هایی را در مورد اطلاعات شخصی با بهانه کمک به یک دوست برای دسترسی پیداکردن وی به چیزی یا بردن یک قرعه‌کشی مطرح می‌کند[۴۵]. یکی از این اقدامات ایجاد شرکت‌ها و سایت‌های کاریابی جعلی برای جمع‌آوری رزومه‌ها و اطلاعات افراد است.

۲-۴-۶- حملات طعمه‌گذاری[۲۴]: طعمه‌گذاری که سیب‌های سر راه هم نامیده می‌شوند، حملاتی هستند که کاربران را تطمیع کرده تا اقدامی که مهندسی اجتماعی می‌خواهد را انجام دهند. مثلاً با رهاکردن فلش مموری در مکانی که فرد هدف در آنجا مستقر است و ترغیب فرد هدف برای وصل کردن آن فلش مموری به سیستم شخصی یا کاری خود، بدافزار یا تروجان روی فلش مموری روی سیستم نصب می‌شود. یا آنها را ترغیب می‌کنند روی لینکی که یک خدمت مجانی را در اختیارشان قرار می‌دهد کلیک کنند. وقتی قربانیان فلش مموری را به رایانه‌هایشان متصل می‌کنند، فلش مموری یا دستگاه ذخیره‌ساز همچون یک اسب تروجان جهانی عمل کرده و به رایانه حمله می‌کند[۴۶].

۳- روش تحقیق

در این تحقیق از روش تحقیق ترکیبی استفاده کردیم چرا که داده‌های کمّی در خصوص سنجش میزان تأثیرگذاری روش‌های مهندسی اجتماعی بر افراد وجود ندارد. بنابراین استفاده از طرح روش‌های ترکیبی ما را قادر می‌سازد تا تحقیق تا آنجا که امکان دارد جامع شود و شواهد تجربی از هر دو پارادایم کمی و کیفی ارائه کند.

۳-۱- مطالعه کیفی

اولین مرحله از تحقیق شامل مطالعه کیفی اکتشافی در مورد نتایج و یافته‌های مطالعات قبلی بوده و زمینه را برای مطالعه کمّی مرحله دوم هموار می‌کند. این مرحله با توصیف تجارب و نیز تحقیقات صورت‌گرفته در خصوص اثرگذاری روش‌های مهندسی اجتماعی بر آسیب‌پذیری کارکنان سروکار داشته و دسته‌بندی‌هایی از انواع روش‌های مهندسی اجتماعی ارائه می‌کند. این طرح تحقیق شامل اطلاعات کتابخانه‌ای، جمع‌آوری اطلاعات از فضای سایبر و نیز انجام مصاحبه‌های نیمه‌باز در قالب مجموعه سؤالات برای اخذ اطلاعات و تجارب مشارکت‌کنندگان است.

سؤال‌های این بخش اصولاً در خصوص چهار موضوع ذیل طراحی شده بود:

پدیده مهندسی اجتماعی، تعریف، ضرورت و اهمیت آن

فرایند اجرای مهندسی اجتماعی و نیازمندی‌های آن

انواع روش‌های مهندسی اجتماعی و کانال اجرای آن

رفتارهای آسیب‌پذیر کارکنان که می‌تواند از روش‌های مهندسی اجتماعی تأثیرپذیر باشند.

افرادی که در این تحقیق مورد مصاحبه قرار گرفتند بر اساس تحقیقات به‌عمل‌آمده، تجربه و دانش و نیز قدرت انعکاس ایده‌ها و نظرات انتخاب شده که البته این موضوع می‌تواند تا اندازه‌ای سوءگیری در تحقیق ایجاد کند؛ اما ازآنجاکه تعداد افراد در دسترس پیرامون این موضوع که علاقه‌مند به شرکت در این مصاحبه بوده، چندان زیاد نبوده و از طرفی قرار نیست این نمونه یک نمونه آماری محسوب شده و همچنین هدف این مرحله از تحقیق (مرحله کیفی) تعمیم‌دادن نتایج مصاحبه به یک جامعه خاص نبوده و صرفاً جهت ارائه نظریات، دانش و تجربه مشارکت‌کنندگان پیرامون موضوع انتخاب شده‌اند، در تحلیل و نتیجه‌گیری تحقیق چندان مشکل‌ساز نیست. هدف اصلی در این مرحله از تحقیق تهیه فهرستی از روش‌ها، بسترها و کانال‌های مورداستفاده مهندسی اجتماعی و رفتارهای آسیب‌زایی است که می‌تواند تحت‌تأثیر این روش‌ها قرار گیرد.

۳-۱-۱- نمونه‌گیری: باتوجه‌به این که نمونه‌های کیفی معمولاً به لحاظ اندازه کوچک بوده در این تحقیق نیز ۱۸ نفر به‌عنوان افراد شرکت‌کننده در مصاحبه از میان کارشناسان حوزه‌های روان‌شناسی، رفتارشناسی، علوم ارتباطات، فضای مجازی و سایبر که آشنا با موضوع بوده انتخاب شدند. ازآنجاکه در تحقیقات کیفی نیازی به اطمینان داشتن از کافی بودن اندازه نمونه برای ارائه برآوردها نبوده، بنابراین در این مرحله انتخاب شمار کوچکی از پاسخ‌دهندگانی که دارای پاسخ‌های مشروح و غنی بوده مناسب تشخیص داده شد.۱۴ نفر از مشارکت‌کنندگان مرد و ۴ نفر از آنها زن بوده و در محدوده سنی بین ۳۵-۶۲ سال بوده‌اند. هرچند مطالب ارائه شده از طرف آنها و مثال‌های ارائه شده از جانب آنها پیرامون مهندسی اجتماعی تقریباً متفاوت بوده اما برایند کلی دسته‌بندی مطالب آنان در خصوص آسیب‌پذیری رفتاری کارکنان نسبت به انواع روش‌های مهندسی اجتماعی ما را به نتایج نسبتاً یکسانی هدایت می‌کرد. می‌توان گفت که فرایند این مرحله از تحقیق به نقطه‌ای رسید که افزایش اندازه نمونه کمکی به اخذ نتایج جدید نمی‌کرد.

[23] Pretexting
[24] Baiting

۳-۱-۲- روش و تحلیل مصاحبه: در این تحقیق از مصاحبه نیمه‌ساختاریافته استفاده شد تا علاوه بر جمع‌آوری پاسخ‌های سؤالات از قبل طراحی شده، امکان جمع‌آوری اطلاعات در خصوص سایر نکات و تجارب مشارکت‌کنندگان نیز وجود داشته باشد. در تحلیل مصاحبه نیز از روش تحلیل محتوا بهره‌برداری شد. تحلیل محتوا می‌تواند ابزار کارا و مؤثری در ارزیابی اطلاعات فراوان ارائه شده توسط مشارکت‌کنندگان باشد.این روش به سازماندهی متون مصاحبه و خلاصه‌کردن و متراکم‌کردن معانی به اشکال کوتاه‌تر کمک می‌کند. مرحله اول شامل مشخص نمودن مطالب یا بیانات اساسی و کلیدی، حذف مطالب تکراری و یا غیرمرتبط و به‌تبع آن ایجاد دسته‌بندی‌هایی برای قراردادن آن مطالب و بیانات در قالب آنها می‌شود. با انجام این مرحله، اهمیت کلی پاسخ‌ها روشن‌تر شده که این موضوع مرحله تفسیر را آسان‌تر می‌سازد. علاوه بر این دسته‌بندی، میزان تکرارپذیری پاسخ‌های مشابه مشخص شده و الگوسازی انجام‌گرفته به ارائه فهم و درک بهتر از داده‌ها با ارزیابی میزان توزیع و تکرار مطالب کمک می‌کند.

۳-۱-۳- روایی و پایایی: هرچند تعداد ۱۸ نفر در مصاحبه شرکت کردند اما اطلاعات جدید نسبتاً اندکی که حاصل شد حکایت از کافی بودن داده‌ها داشت و به نقطه‌ای رسید که نیازی به مصاحبه‌های بیشتر احساس نشد.

در این تحقیق مطالب جمع‌آوری شده از مصاحبه‌ها به‌درستی پدیده مهندسی اجتماعی را توصیف می‌کنند زیرا مطالب حاصل از فرایند دسته‌بندی با نوشته‌ها و یافته‌های قبلی تا حد زیادی سازگار بود. علاوه بر این، بخشی از اطلاعات ارائه شده، تجارب واقعی، معتبر و شخصی افراد از پدیده مهندسی اجتماعی بوده است.

تکرارپذیری یا تعمیم‌پذیری جزو وظایف محقق در این مرحله از تحقیق نبوده چرا که این مرحله از تحقیق (مطالعه کیفی) به دنبال تعمیم‌دادن نتایج به یک جمعیت خاص نیست. علاوه بر این، یافته‌های تحقیق بازتاب درستی از پدیده مهندسی اجتماعی است چرا که مطالب حاصله از این تحقیق با یافته‌ها و نتایج قبلی در این حوزه منطبق است.

۳-۱-۴- یافته‌ها: هرچند در خصوص موضوع مهندسی اجتماعی و موارد فوق اختلافات جزئی میان کارشناسان و همچنین محققانی که دررابطه‌با این موضوع تحقیق کرده بودند در خصوص دسته‌بندی‌های صورت‌گرفته وجود داشت اما جدول (۱) برآورد حاصل از مجموعه نظرات مشارکت‌کنندگان در مصاحبه و نیز تحقیقات صورت‌گرفته قبلی است که برای نشان‌دادن و یکپارچه نمودن انواع روش‌های مهندسی اجتماعی و یکپارچه‌سازی انواع آسیب‌پذیری‌های رفتاری کارکنان در برابر روش‌های مهندسی اجتماعی مورداستفاده قرار گرفته است.

بخش افقی جدول مربوط به انواع روش‌های مهندسی اجتماعی است که ۲۳ روش از جانب اکثر کارشناسان به‌عنوان روش‌های مورداستفاده مهندسان اجتماعی مورد تأیید قرار گرفت که در جدول یک مشخص شده است.

در بخش عمودی جدول نیز انواع کانال‌های ارتباطی، عامل ارتباط، روش و آسیب‌پذیری به تفکیک ارائه شده که کانال‌های مورداستفاده، عامل ارتباطی و نوع روش و آسیب‌پذیری مرتبط با هر روش (در بخش افقی) با رنگ مشکی پر شده است.

منظور از کانال ارتباطی بستر و فضایی است که مهندسان اجتماعی از این فضا و بستر استفاده کرده تا با استفاده از روش‌های مهندسی اجتماعی در این فضا، قربانیان خود را فریب دهند که شامل ایمیل، پیام رسانه‌ای فوری، تلفن، شبکه‌های اجتماعی، فضاهای ابری، وب‌سایت‌ها، ارتباطات چهره به چهره یا فیزیکی، پنجره‌های پاپ‌آپ و برنامه‌های موبایلی است.

عامل ارتباط نیز به دودسته انسان و نرم‌افزار تقسیم شده که روش‌های مهندسی اجتماعی یا از عامل انسان یا از نرم‌افزارها یا از هر دو بهره‌برداری می‌کنند. هرکدام از روش‌ها در یکی از انواع فیزیکی، فنی، اجتماعی و فنی - اجتماعی گنجانده شده که در جدول یک نیز با رنگ مشکی مشخص شده است.

در ارتباط با انواع آسیب‌پذیری‌های انسان در برابر روش‌های مهندسی اجتماعی نیز در نهایت ۱۴ عنوان آسیب‌پذیری ذکر شده در جدول یک از طرف اکثر کارشناسان تأیید گردید. سوءاستفاده روش‌های مهندسی اجتماعی از هرکدام از آسیب‌پذیری‌ها نیز با رنگ مشکی در جدول مشخص شده است.

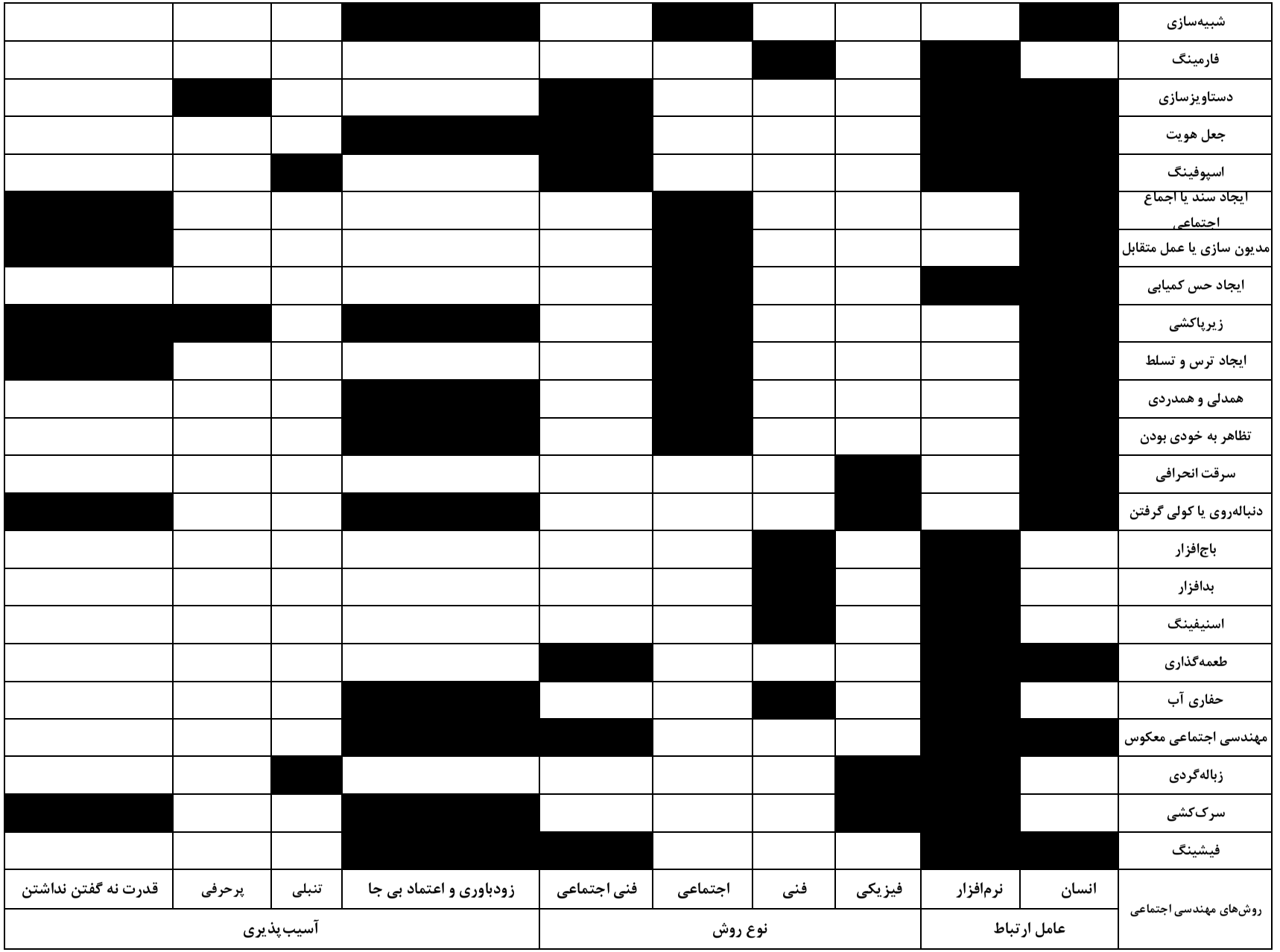
۳-۲- مطالعه کمّی

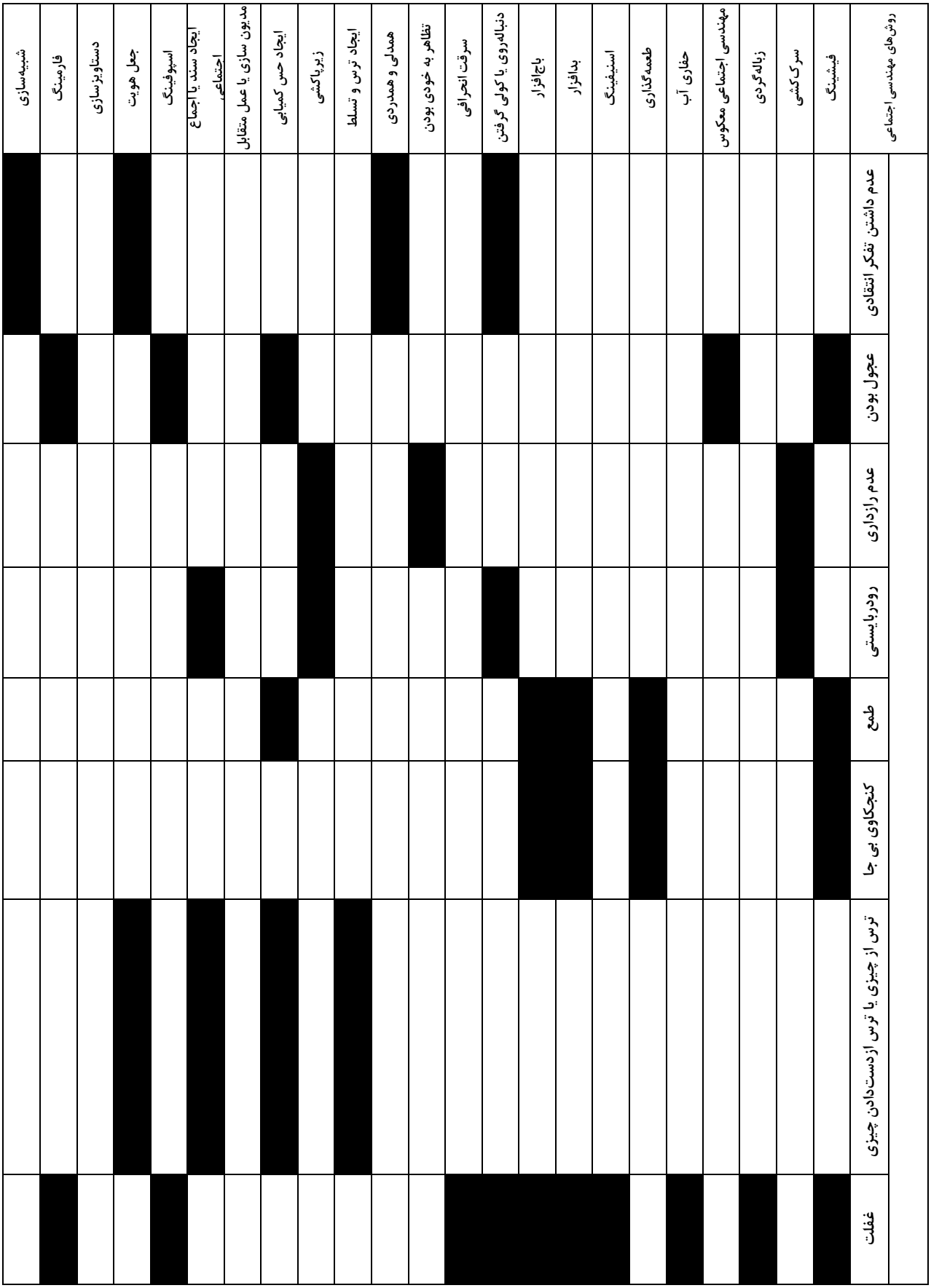
نتایج مرحله اول زمینه را برای طراحی مقیاس اثرگذاری روش‌های مهندسی اجتماعی بر آسیب‌پذیری کارکنان در این مرحله از تحقیق فراهم کرد. هدف این مرحله از تحقیق آن است که روشی عینی را در سنجش میزان آسیب‌پذیری کارکنان نسبت به روش‌های مهندسی اجتماعی، طراحی، اجرا و ارزیابی نماید و کاوش بیشتری در تجارب مربوط به مهندسی اجتماعی با استفاده از ارتباط آن با آسیب‌پذیری‌هایی که منجر به سوءاستفاده از کارکنان شده انجام دهد. روش کمّی این مرحله از تحقیق از پرسش‌نامه به‌عنوان ابزار پیمایش بهره برده است.

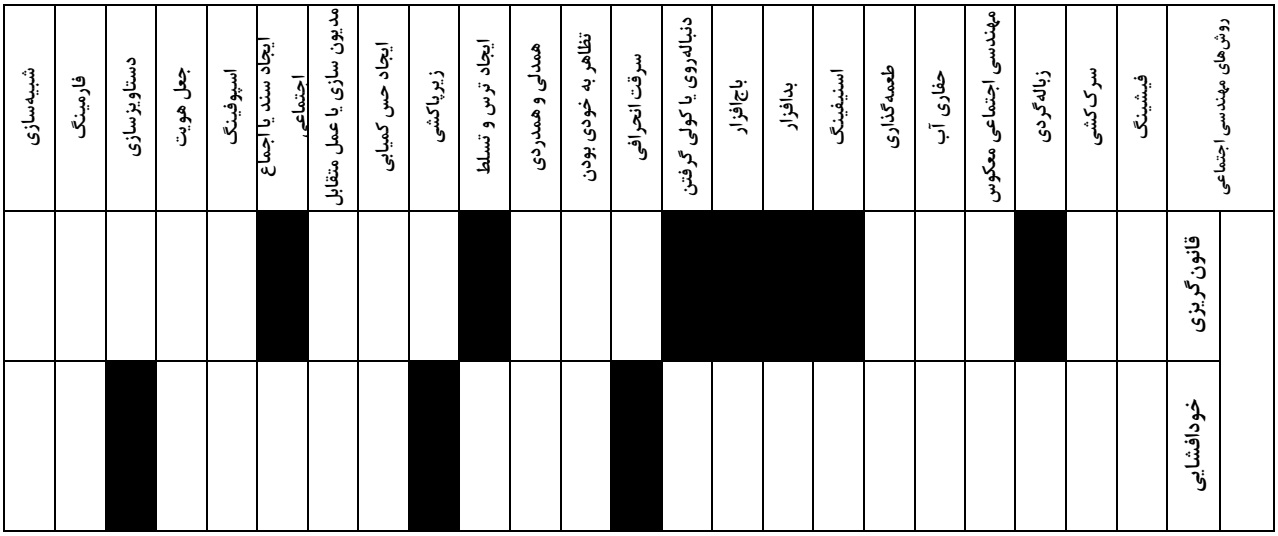
ما باتوجه‌به گزاره‌های مورداستفاده در پرسش‌نامه آسیب‌پذیری کارکنان را در برابر انواع روش‌های مهندسی اجتماعی فوق‌الذکر مورد سنجش قرار داده، سپس با تعیین میانگین وزن‌دهی داده شده به هرکدام از روش‌ها، میانگین مجموعه روش‌های مربوط به هر دسته (مثل روش‌های فنی) را به دست آورده تا میزان آسیب‌پذیری نسبت به هرکدام از انواع (فنی، فیزیکی، اجتماعی، فنی - اجتماعی) مشخص گردد.

جدول (۱). انواع روش‌های مهندسی اجتماعی به تفکیک کانال ارتباطی، عامل ارتباط، نوع و آسیب‌پذیری مرتبط

روش‌های مهندسی اجتماعی	کانال‌های ارتباطی									
	ایمیل	پیام‌رسان فوری	تلفن	شبکه اجتماعی	فضای ابری	وب‌سایت	فیزیکی	پنجره‌های پاپ‌آپ	برنامه‌های موبایلی	
فیشینگ	■	■				■		■		
سرک‌کشی							■			
زباله‌گردی							■			
مهندسی اجتماعی معکوس	■	■	■			■	■		■	
حفاری آب						■				
طعمه‌گذاری	■	■	■		■	■				
اسنیفینگ		■	■		■					
بدافزار		■		■		■		■		
باج‌افزار	■	■		■		■		■		
دنباله‌روی یا کولی گرفتن							■			
سرقت انحرافی							■			
تظاهر به خودی بودن				■			■			
همدلی و همدردی				■			■			
ایجاد ترس و تسلط				■			■			
زیرپاکشی			■				■			
ایجاد حس کمیابی	■	■				■		■		
مدیون سازی یا عمل متقابل							■			
ایجاد سند یا اجماع اجتماعی		■		■			■			
اسپوفینگ	■					■				
جعل هویت	■	■	■	■			■		■	
دستاویزسازی	■		■				■		■	
فارمینگ						■				
شبیه‌سازی				■			■		■	


شبیه‌سازی
فارمینگ
دستاویزسازی
جعل هویت
اسپوفینگ
ایجاد سند یا اجماع اجتماعی
مدیون سازی یا عمل متقابل
ایجاد حس کمیابی
زیرپاکشی
ایجاد ترس و تسلط
همدلی و همدردی
تظاهر به خودی بودن
سرقت انحرافی
دنباله‌روی یا کولی گرفتن
باج‌افزار
بدافزار
اسنیفینگ
طعمه‌گذاری
حفاری آب
مهندسی اجتماعی معکوس
زباله‌گردی
سرک‌کشی
فیشینگ
روش‌های مهندسی اجتماعی
انسان
نرم‌افزار
فیزیکی
فنی
اجتماعی
فنی اجتماعی
زودباوری و اعتماد بی جا
تنبلی
پرحرفی
قدرت نه گفتن نداشتن
عامل ارتباط
نوع روش
آسیب‌پذیری


روش‌های مهندسی اجتماعی
عدم داشتن تفکر انتقادی
عجول بودن
عدم رازداری
رودربایستی
طمع
کنجکاوی بی جا
ترس از چیزی یا ترس ازدست‌دادن چیزی
غفلت
فیشینگ
سرک کشی
زباله‌گردی
مهندسی اجتماعی معکوس
حفاری آب
طعمه‌گذاری
اسپیفینگ
بدافزار
باج‌افزار
دنباله‌روی یا کولی گرفتن
سرقت انحرافی
تظاهر به خودی بودن
همدلی و همدردی
ایجاد ترس و تسلط
زیرپاکشی
ایجاد حس کمبابی
مدیون سازی یا عمل متقابل
ایجاد سند یا اجماع اجتماعی
جعل هویت
اسپوفینگ
دستاویزسازی
فارمینگ
شبیه‌سازی



۳-۲-۱- طراحی پرسش‌نامه: پرسش‌نامه‌ای به‌عنوان ابزار پیمایش جهت جمع‌آوری داده‌های مربوط به رفتار و واکنش و پاسخ افراد در برابر روش‌های مهندسی اجتماعی و مسائل جمعیت‌شناختی طراحی شد. بخش اول این پیمایش شامل ۵۰ سؤال بود که شامل گزاره‌های مربوط به رفتارهای افراد در برخورد با روش‌های مهندسی اجتماعی است. بخش دوم مربوط به اطلاعات جمعیت‌شناسی کارکنان بود که شامل جنسیت، وضعیت تأهل، میزان تحصیلات و ... می‌شود. پاسخ‌دهندگان پاسخ‌هایشان را از طریق یک مقیاس لیکرت پنج امتیازی ثبت می‌کردند به‌طوری‌که شماره یک برابر با کاملاً مخالف و شماره پنج معادل کاملاً موافق می‌شد. هر آیتم به‌صورت یک عبارت اخباری ارائه شده که از پاسخ‌های ارائه شده توسط پاسخ‌دهندگان نشئت‌گرفته که میزان موافقت با آن عبارت را مشخص می‌کنند. برخی از آیتم‌های پرسش‌نامه می‌توانست چند روش مهندسی اجتماعی را پوشش دهد اما در نهایت به یکی از روش‌ها نسبت داده شد که این موضوع تأثیر چندانی در نتیجه‌گیری پایانی که سنجش میزان آسیب‌پذیری کلی کارکنان نسبت به روش‌های مهندسی اجتماعی است ندارد. آیتم‌های چندگانه (عبارات اخباری) برای سنجش هرکدام از این آسیب‌پذیری‌ها ایجاد شد. این آیتم‌های چندگانه هم از محتوای موجود در کتاب‌های نگارش شده و تحقیقات صورت‌گرفته و هم از موضوعات و مطالبی که از مصاحبه‌های قبلی به‌دست‌آمده نشئت‌گرفته است.

در خصوص سنجش هرکدام از روش‌ها یک یا چند آیتم به فراخور به‌کاررفته تا میزان آسیب‌پذیری آن کارمند نسبت به آن روش مشخص گردد. در نهایت با میانگین‌گیری امتیازات ارائه شده به آیتم‌های یک روش، میزان آسیب‌پذیری در برابر آن روش مشخص خواهد شد. در ادامه نیز با معدل گیری هرکدام از میانگین‌های به‌دست‌آمده از هرکدام از انواع روش‌ها (فنی، فیزیکی، اجتماعی، فنی - اجتماعی) میزان آسیب‌پذیری کارکنان نسبت به هر دسته به دست خواهد آمد.

۳-۲-۲- روایی و پایایی: پایایی ابزارهای پیمایش از طریق فرایند پیش آزمایش افزایش می‌یابد. هدف پیش آزمایش این است که ساختار پرسش‌نامه، جمله‌بندی سؤالات و توالی سؤالات را آزمایش می‌کند. بنابراین بعد از انجام پیش آزمایش که ارائه پرسش‌نامه به ۲۳ نفر از افراد به‌صورت آزمایشی برای ارزیابی پرسش‌نامه بود، برخی از پرسش‌ها جمله‌بندی مجدد شده و ساختارهای آنها واضح‌تر و روشن‌تر شدند.

در ارتباط با حداکثرسازی اعتبار مقیاس در این مطالعه، آیتم‌ها توسط چند نفر از متخصصین حوزه‌های ارتباطات، روان‌شناسی، رایانه و فضای مجازی مورد بازبینی قرار گرفت و در مرحله اصلاح پایانی برخی آیتم‌ها اصلاح شدند. برخی آیتم‌ها نیز باتوجه‌به آنکه به نظر کارشناسان چندان نمی‌توانست نمایانگر میزان آسیب‌پذیری کارکنان در برابر آن روش خاص باشند حذف و آیتم‌های دیگری جایگزین گردید.

۳-۲-۳- نمونه‌گیری: در این بخش سعی شد تا از میان کارکنان شهرداری تهران و مناطق ۲۲ گانه آن افرادی را به‌تصادف انتخاب کرده تا میزان آسیب‌پذیری آنها را مورد سنجش قرار دهیم چرا که ممکن بود نوع کار، ارباب‌رجوع، تخصص، مسائل شغلی و ... در میان کارکنان مناطق ۲۲ گانه شهرداری تا حدودی متفاوت باشد. بنابراین محقق پس از انتخاب تصادفی این افراد، پرسش‌نامه را در اختیار ۱۳۶۲ نفر از آنان قرار داد. 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) پرسش‌نامه برایشان ارسال گردید. در پرسش‌نامه ارسال شده هدف از انجام این کار و نیز نحوه

پاسخ‌دهی به آن توضیح داده شده بود. تعداد افرادی که پاسخ‌نامه را کامل نموده و آن را ارسال نموده بودند ۱۳۳۸ نفر بود که از میان آنها ۱۳۲۲ نفر به طور کامل به پرسش‌نامه پاسخ داده و با بررسی صورت‌گرفته مشخص شد که اطلاعات مندرج در پرسش‌نامه از جانب برخی از افرادی که به پرسش‌نامه پاسخ داده بودند (۱۶ نفر) چندان معتبر نبوده است و بنابراین جمعیت نمونه موردنظر به ۱۳۲۲ نفر تقلیل یافت که از همه مناطق ۲۲گانه تهران در این جمعیت نمونه به تعداد تقریباً یکسان حضور داشتند.

۳-۲-۴- فرایند تحلیل داده‌ها: کل اطلاعات دریافتی از پاسخ‌دهندگان کدبندی شده و درون نرم‌افزار SPSS تغذیه شد.برای تحلیل داده‌ها اول، آمارهای توصیفی برای تمامی متغیرهای مهندسی اجتماعی و متغیرهای جمعیت‌شناختی ایجاد شد تا نرمال بودن متغیرها مشخص شود و پاسخ‌های ارائه شده به هر عبارت در خصوص آسیب‌پذیری در برابر روش‌های مهندسی اجتماعی مورد محاسبه و تحلیل قرار گرفت و سپس باتوجه‌به دسته‌بندی صورت‌گرفته در خصوص روش‌ها، آمارهای مربوط به وضعیت هرکدام از دسته‌ها مشخص گردید.

۳-۲-۵- نتایج: 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 سوءگیری 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. در خصوص درآمد نیز، اکثر پاسخ‌دهندگان دارای درآمد بین ۷ تا ۱۰ میلیون تومان بوده‌اند.

۴- نتایج

۴-۱- آسیب‌پذیری نسبت به روش‌های مهندسی اجتماعی:

باتوجه‌به پاسخ‌های ارائه شده توسط مشارکت‌کنندگان میانگین وزنی هرکدام از آیتم‌های ارائه شده مشخص گردید که هر چقدر این مقدار به عدد ۵ نزدیک‌تر باشد، مشخص است که میزان آسیب‌پذیری کارکنان نسبت به آن آیتم بیشتر بوده است. لازم به ذکر است که باتوجه‌به نظر کارشناسان وزن تمامی آیتم‌ها از جهت اهمیت و تأثیرگذاری بر آسیب‌پذیری در پرسش‌نامه و تحلیل نتایج یکسان در نظر گرفته شده است.

در جدول شماره ۲ معدل میانگین وزنی ارائه شده به آیتم‌های مربوط به یک روش آورده شده است. در خصوص روش‌هایی که در پرسش‌نامه دارای یک آیتم بوده، میانگین وزنی همان آیتم، میانگین کلی مربوط به آن روش است که در جدول شماره ۲ به ترتیب از کمترین تا بیشترین آورده شده است.

جدول (۲). معدل میانگین وزنی ارائه شده به روش‌ها

رتبه	روش	میانگین وزنی
۱	حفاری آب	۴/۵
۲	همدلی و همدردی	۴/۰۹
۳	اسپوفینگ	۳/۷۴
۴	ایجاد ترس و تسلط	۳/۷۴
۵	شبیه‌سازی	۳/۶۸
۵	فارمینگ	۳/۵۹
۷	زیرپاکشی	۳/۵۲
۸	ایجاد سند یا اجماع اجتماعی	۳/۴۱
۹	فیشینگ	۳/۴۱
۱۰	اسنیفینگ	۳/۳۷
۱۱	دستاویزسازی	۳/۳۱
۱۲	تظاهر به خودی بودن	۳/۲۶
۱۴	بدافزار	۲/۹۲
۱۴	زباله‌گردی	۲/۸۷
۱۵	باج‌افزار	۲/۷۹
۱۶	کولی گرفتن	۲/۶۷
۱۷	جعل هویت	۲/۵۷
۱۸	ایجاد حس کمیابی	۲/۴۶
۱۹	طعمه‌گذاری	۲/۴۶
۲۰	مدیون سازی	۲/۳۹
۲۱	مهندسی اجتماعی معکوس	۱/۸۶
۲۲	سرک‌کشی	۱/۸۳
۲۳	سرقت انحرافی	۱/۰۴

همان‌طور که در جدول ۲ مشخص است مشارکت‌کنندگان نسبت به سرقت انحرافی کمترین آسیب‌پذیری و نسبت به روش حفاری آب بیشترین آسیب‌پذیری را دارند. بعد از حفاری آب نیز نسبت به روش‌های اسپوفینگ، ایجاد ترس و تسلط و شبیه‌سازی دارای بیشترین آسیب‌پذیری هستند.

۴-۲- آسیب‌پذیری نسبت به نوع روش

در جدول شماره ۳ میانگین وزنی مربوط به هر دسته باتوجه‌به معدل کلی به‌دست‌آمده از میانگین کسب شده از هرکدام از روش‌ها آورده شده است. به‌عنوان‌مثال حاصل میانگین وزنی پاسخ‌های ارائه شده نسبت به روش‌های فیشینگ، مهندسی اجتماعی معکوس، طعمه‌گذاری، اسپوفینگ، جعل هویت و دستاویزسازی به‌عنوان میانگین وزنی ارائه شده مربوط به نوع روش‌های فنی - اجتماعی در نظر گرفته می‌شود. در خصوص روش‌های مرتبط با سایر انواع هم، این میانگین وزنی ارائه شده که در جدول شماره ۳ از کمترین آسیب‌پذیری نسبت به نوع روش تا بیشترین آن مرتب شده است.

جدول شماره (۳).میانگین وزنی انواع کلی روش‌های مهندسی اجتماعی

رتبه	نوع روش	میانگین وزنی
۱	فیزیکی	۲/۱۰
۲	فنی - اجتماعی	۲/۸۹
۳	اجتماعی	۳/۳۱
۴	فنی	۳/۴۳

۵- نتیجه‌گیری و پیشنهادات

به نظر می‌رسد باتوجه‌به یافته‌ها، می‌توان نتیجه گرفت که کارکنان نسبت به روش‌های فنی به این دلیل که در آنها از روش‌های پیچیده‌تر فنی و سایبری استفاده شده و نیز نیازمند آشنایی کارکنان با فضای مجازی و آسیب‌های آن بوده، آسیب‌پذیری بیشتری دارند. از طرفی نسبت به روش‌های اجتماعی که بیشتر در تعاملات چهره‌به‌چهره رخداده نیز آسیب‌پذیر هستند.

باتوجه‌به این نتیجه و نیز دسته‌بندی انجام شده در خصوص ارتباط هرکدام از روش‌ها با نوع آسیب‌پذیری‌ها، زودباوری و اعتماد بی‌جا، نداشتن تفکر انتقادی، تنبلی، عجول بودن، غفلت، نداشتن قدرت نه گفتن، ترس از چیزی یا ترس ازدست‌دادن چیزی و قانون‌گریزی جزو آسیب‌پذیرترین رفتارهای کارکنان مشارکت‌کننده محسوب می‌شوند.

فرهنگ امنیتی سازمان به کارایی برنامه امنیت اطلاعاتش کمک می‌کند. هنگامی که فرایندهای امنیتی در فرهنگ یک سازمان به طور کامل نهادینه شود و سطح بالایی از آگاهی امنیتی وجود داشته باشد، برنامه امنیت اطلاعات مؤثرتر خواهد بود. تیم مدیریت یک سازمان باید امنیت اطلاعات را درک کرده و از آن حمایت کند و منابع مناسبی را برای توسعه، اجرا و نگهداری از برنامه امنیت اطلاعات فراهم کند. نتیجه این درک و حمایت، برنامه‌ای است که در آن هم مدیریت و هم کارکنان متعهد به ادغام این برنامه در فرایندهای کاری هستند[۴۷].

امنیت اطلاعات موضوع بسیار حائز اهمیتی است و بسیاری از کاربران نمی‌توانند میزان اهمیت آن را درک کنند یا حتی اگر بتوانند آن را درک کنند تنها به‌عنوان نوش‌دارو پس از مرگ سهراب است. هدف اجرای امنیت اطلاعات دفاع در برابر تهدیدات احتمالی است که اطلاعات سازمان را تهدید می‌کند. امنیت اطلاعات برای سازمان‌ها و شرکت‌ها الزامی است و باید تهدیدات مرتبط با امنیت اطلاعات و آسیب‌پذیری سیستم‌ها را به حداقل برسانند[۴۸]. جریان کنترل اطلاعات میان سازمان‌ها یا اشخاص، باعث حفظ و رشد شرکت‌ها و سازمان‌ها می‌شود[۴۹]. ایجاد یک برنامه تهدیدات کارکنان می‌تواند به سازمان‌ها در کشف، پیشگیری و پاسخ به تهدیداتی که از جانب کارمندانی که عامدانه یا ناخواسته دست به انجام این کار می‌زنند کمک کند. لازم به ذکر است که قلمرو و توسعه این برنامه باتوجه‌به بودجه، اندازه، فرهنگ و صنعت حاکم بر سازمان ممکن است بسیار متفاوت باشد.

راهکارهای ارائه شده در خصوص مقابله با پدیده مهندسی اجتماعی اصولاً شامل دو بخش انسان‌محور و رایانه محور (فناوری محور) است. روش‌های انسان‌محور به تصمیمات ذهنی انسان‌ها وابسته است[۵۰]. آموزش کارکنان در خصوص روش‌ها و روش‌های مقابله با مهندسی اجتماعی و نیز ایجاد فرهنگ امنیتی مناسب در سازمان از جمله اقدامات لازم در خصوص پیشگیری از وقوع مهندسی اجتماعی است. روش‌های فناوری محور یا رایانه محور نیز مبتنی بر ایجاد زیرساخت و قوانین و مقررات لازم در یک سازمان برای پیشگیری از وقوع مهندسی اجتماعی است. مثلاً ایجاد چرخه درست و منطقی دسترسی به اطلاعات، قوانین مربوط به نظارت بر داده‌ها و ایجاد تمهیدات حفاظتی و نظارتی در سازمان را می‌توان از جمله اقدامات فناوری محور قلمداد کرد.

۶- مراجع

[1] K.Mitnick,W.Simon and S.Wozniak,"The Art of Deception: Controlling the Human Element of Security", NJ: Wiley, 2002.

[2]Social Engineer, "Security though education", Retrieved March 29, 2016, from The Social Engineering Framework: http://www.social-engineer. org/framework/psychological, 2016.

[3] Symantec Corporation,"INTERNET SECURITY THREAT REPORT",Retrieved 31 03,2016,from http://www.symantec.com/content/en/us/enterprise/other_r

International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, pp.1–10, 2016.

[20] Kaspersky, "Pharming definition", https://www.kaspersky.com/resource-center/definitions/pharming, 2021.

[21] E.Aharoni, "What is a Watering Hole attack and how to prevent them" https://blog.cymulate.com/watering-hole-attack-dont-drink-water, 2021

[22] N.Pokrovskaia, "Social engineering and digital technologies for the security of the social capital'development", In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, pp.16–19, 2017.

[23] K.Krombholz, H.Hobel, M.Huber and E.Weippl, "Advanced social engineering attacks". J. Inf. Secur. Appl, pp. 113–122, 2014

[24] K.Axelton, "what is shoulder surfing" https://www.experian.com/blogs/ask-experian/what-is-shoulder-surfing/, 2020

[25] L.Xiangyu, L.Qiuyang and S.Chandel, "Social engineering and Insider threats", In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, pp.25–34, 2017.

[26] Y.Diogenes and E.Ozkaya, "Cybersecurity –Attack and Defense Strategies", https://www.oreilly.com/library/view/cybersecurity-attack/9781788475297/6a6d16cf-64bb-411e-bba2-ecbd10ad2d88.xhtml, 2021

[27] P.Patil and P.Devale, "A literature survey of phishing attack technique", Int. J. Adv. Res. Comput. Commun. Eng, pp.198–200, 2016.

[28] S.Granger, "Social engineering fundamentals", www.securityfocus.com/infocus/1527 and 1533, 2006.

[29] S.A.Moosavi, "Social Engineering,Art of Psychological War, Human Hacking,Persuation and Deception", Tehran.Nasleroshan, 2020.(In Persian)

[30] S.Aslany and H.Eskandary, "An overview of the Importance of Compassion in Community Security", Rooyesh-e-Ravanshenasi, vol.7, no.11, Serial no.32, pp.341-354, 2019. (In Persian)

[31] G.Seidman, "Why Do We Like People Who Are Similar to Us?", https://www.psychologytoday.com/us/blog/close-encounters/201812/why-do-we-people-who-are-similar-us, 2021.

[32] R.Cialdini, "Influence: The Psychology of Persuasion", New York,Harper Business, 2006

[33] US Commodity Futures Trading Commission, "Foreign Currency Trading (Forex) Fraud", https://www.cftc.gov/ConsumerProtection/FraudAwarenessPrevention/CFTCFraudAdvisories/fraudadv_forex.html, 2019

[34] D.Gragg, "A Multi-Level Defense Against Social Engineering", SANS Institute, InfoSec Reading Room, pp.13-18, 2003.

[35] S.Stasiukoni, " Social Engineering, the USB Way", http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634, 2013.

esources/bistr_main_report_v19_21291018.en-us.pdf, 2014.

[4] R.Ballagas, M.Rohs, J.Sheridan and J.Borchers, "Byod: Bring your own device", In Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp, 2004.

[5] W.Shen, "Active Social Engineering Defense (ASED)", Defense Advanced Research Projects Agency Program Information. Accessed February 1, 2019. https://www.darpa.mil/program/active-social engineering-defense, 2019.

[6] A.Chantler and R.Broadhurst, "Social Engineering and Crime Prevention in Cyberspace", Queensland University of Technology, 2006.

[7] C.Hadnagy, "Social Engineering: The Art of Human Hacking", NJ: Wiley, 2011.

[8] T.Qin and J.Burgoon, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. Intelligence and Security Informatics", IEEE, pp. 152–159, 2007.

[9] N.Verma, "Social Engineering: A Means to Violate a Computer System", Publisher Global Vision Publishing House, 2011.

[10] K.D.Mitnick, "The Art of Deception - Controlling the Human Element of Security", Indiana,Wiley Publishing, p.16, 2003.

[11] B.Oosterloo, "Managing Social Engineering Risk", University of Twente, 2008

[12] N.Pavkovic and L.Perkov, "Social Engineering Toolkit—A systematic approach to social engineering", 34th IEEE International Convention MIPRO, Opatija, Croatia, pp.1485–1489, 2011.

[13] A.V.Grebmer, "Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security". Publisher. BoD – Books on Demand. pp.58-74, 2008.

[14] M.Erbschloe, "Social Engineering-Hacking systems,nations and societies", Translated by Seyyedhasan Hoseiny, Tehran, Sabah, 1400.(In Persian)

[15] H.Kim, D.Yoo, J.Kang and Y.Yeom, "Dynamic ransomware protection using deterministic random bit generator", In Proceedings of the IEEE Conference on Applications, Information and Network Security, Miri, Malaysia, pp.1–6, 2017.

[16] S.Wang, S.Zhu and Y.Zhang, "Blockchain-based mutual authentication security protocol for distributed RFID systems", In Proceedings of the IEEE Symposium on Computers and Communications, Natal, Brazil, pp.74–77, 2018.

[17] L.Segovia, F.Torres, M.Rosillo, E.Tapia, F.Albarado and D.Saltos, "Social engineering as an attack vector for ransomware", In Proceedings of the Conference on Electrical Engineering and Information Communication Technology, Pucon, Chile, pp.1–6, 2017.

[18] D.F.Sittig and H.Singh, "Asocio-technical approach to preventing, mitigating and recovering from ransomware attacks", Appl. Clin. Inform, pp. 624–632, 2016.

[19] B.Arya and K.Chandrasekaran, "A client-side anti-pharming (CSAP) approach", In Proceedings of the IEEE

[36] L.J.Janczewski and A.Colarik, "Cyber Warfare and Cyber Terrorism", Pennsylvania, Idea Group Inc, 2008.

[37] K.Beckers, S.Pape, "A serious game for eliciting social engineering security requirements", In Proceedings of the International Requirements Engineering Conference, Beijing, China,pp.16–25, 2016.

[38] L.Peotta, M.D.Holtz, B.M.David, F.G.Deus and R.T.De Sousa, "A formal classification of internet banking attacks and vulnerabilities",Int. J. Comput. Sci. Inf. Technol. 3,pp.186–197, 2011.

[39] G.Ho, A.Sharma, M.Javed, V.Paxson and D.Wagner, "Detecting credential spearphishing in enterprise settings", In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, pp.469–485, 2017.

[40] Techopedia Dictionary, "Whaling Definition", https://www.techopedia.com/definition/28643/whaling, 2016.

[41] E.O.YeboahBoateng and P.M.Amanor, "Phishing,SMiShing&Vishing:Anassessment of threats against mobile devices" J. Emerg. Trends Comput. Inf. Sci. 5, pp.297–307, 2014

[42] H.Tu, A.Doupé, Z.Zhao and G.J.Ahn, "Everyone hates robocalls: A survey of techniques against telephone spam", In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA. pp. 320–338, 2016.

[43] T.Braun, B.C.Fung, F.Iqbal and B.Shah, "Security and privacy challenges in smart cities", Sustain. Cities Soc, pp.39,499-507, 2018

[44] Sophos, "Sophos facebook id probe shows 41% of users happy to reveal all to potential identity thieve". http://www.sophos.com/en-us/press, 2007

[45] I.Ghafir, "Social engineering attack strategies and defence approaches", In Proceedings of the IEEE International Conference on Future Internet of Things and Cloud, Vienna, Austria,PP.1–5, 2016

[46] G.Costantino, A.La Marra, F.Martinelli, and I.Matteucci, "CANDY: A social engineering attack to leak information from infotainment system", In Proceedings of the IEEE Vehicular Technology Conference, Porto, Portugal, pp.1– 5, 2018.

[47] Federal Financial Institutions Examination Council, "Security Culture", https://ithandbook.ffiec.gov/it-booklets/information-security/i-governance-of-the-information-security-program/ia-security-culture.aspx, 2019

[48] S.Abraham, "An overview of social engineering malware: Trends, tactics, and implications", Technology in Society, p.183, 2010.

[49] D.Ashenden, "Information Security management: A human challenge?", Information Security Technical Report, 2008.

[50] R.Heartfield and G.Loukas, " A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks", ACM Comput, Surv, pp.48, 1–37, 2016.